EXHIBIT A
Redacted Version of Document Sought to be Sealed

Mark C. Mao, CA Bar No. 236165
Beko Reblitz-Richardson, CA Bar No. 238027
BOIES SCHILLER FLEXNER LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
Fax: (415) 293-6899
mmao@bsfllp.com
brichardson@bsfllp.com

Jesse Panuccio (admitted *pro hac vice*)
BOIES SCHILLER FLEXNER LLP
1401 New York Ave, NW
Washington, DC 20005
Tel.: (202) 237-2727
Fax: (202) 237-6131
jpanuccio@bsfllp.com

Amanda K. Bonn, CA Bar No. 270891
SUSMAN GODFREY L.L.P
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA. 90067
Tel: (310) 789-3100
Fax: (310) 789-3150
abonn@susmangodfrey.com

John A. Yanchunis (admitted *pro hac vice*)
Michael F. Ram, CA Bar No. 104805
Ryan J. McGee (admitted *pro hac vice*)
Ra Amen (admitted *pro hac vice*)
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
rmcgee@forthepeople.com

William S. Carmody (admitted *pro hac vice*)
Shawn Rabin (admitted *pro hac vice*)
Steven M. Shepard (admitted *pro hac vice*)
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019-6023
Tel.: (212) 336-8330
Fax: (212) 336-8340
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

ANIBAL RODRIGUEZ, JULIEANNA MUNIZ, ELIZA CAMBAY, SAL CATALDO, EMIR GOENAGA, JULIAN SANTIAGO, HAROLD NYANJOM, KELLIE NYANJOM, and SUSAN LYNN HARVEY, individually and on behalf of all other similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 3:20-cv-04688-RS

SECOND AMENDED COMPLAINT

CLASS ACTION FOR
(1) BREACH OF CONTRACT;
(2) INVASION OF PRIVACY ACT VIOLATIONS, CAL. PENAL CODE § 631;
(3) VIOLATIONS OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA"), CAL. PENAL CODE §§ 502 *ET SEQ.*
(4) INVASION OF PRIVACY;
(5) INTRUSION UPON SECLUSION

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiffs Anibal Rodriguez, JulieAnna Muniz, Eliza Cambay, Sal Cataldo, Emir Goenaga, Julian Santiago, Harold Nyanjom, Kellie Nyanjom, and Susan Lynn Harvey, individually and on behalf of all others similarly situated, file this Second Amended Class Action Complaint against defendant Google LLC ("Google" or "Defendant"), and in support state the following.

INTRODUCTION

"*I want people to know that everything they're doing online is being watched, is being tracked, is being measured. Every single action you take is carefully monitored and recorded.*"

-Jeff Seibert; Former Head of Consumer Product of Twitter[1]

1. This case is about Google's surreptitious interception and collection of consumers' highly personal browsing histories on their mobile devices, whenever consumers use certain software applications ("apps") that have incorporated Google code. Google did this without notice or consent, where Plaintiffs had turned off a Google feature called "Web & App Activity." Google had promised that by turning off this feature, users would stop Google from saving their web and app activity data, including their app-browsing histories. Google's promise was false.

2. Google has said, over and over again, that it values privacy and gives users control. The truth is just the opposite. Google continues to track users and collect their data even after users follow Google's instructions on how to stop that tracking and collection. What Google calls its privacy "controls" are ruses. These Google features are intended to lull users—along with regulators, legislators, and app developers—into a false sense of control and privacy. No matter what users do, Google never stops intercepting, collecting, tracking, and using users' app-browsing data.

3. Google surreptitiously collected users' personal data from their mobile devices using software scripts embedded in Google's Firebase SDK development platform. Third-party software developers then used Firebase SDK to build their apps (as Google coerced them to do).

[1] *The Social Dilemma*, NETFLIX (Jan. 2020), https://www.netflix.com/title/81254224?s=i&trkid=13747225.

Users downloaded and used those apps to communicate with third parties (e.g., The New York Times app allows users to communicate with The New York Times) through their mobile devices. Unknown to users, the Firebase SDK scripts still copied users' communications and transmitted them to Google's servers through the users' devices, to be saved and used by Google for Google's purposes. Google did all this even if users switched off Google's "Web & App Activity" feature, without providing any notice or obtaining any consent.

4. Google repeatedly told its users that if they "turn off" the "Web & App Activity" feature, then that would stop Google from "sav[ing]" the users' app data. Similarly, Google presented such settings to their business partners as device level controls, including by requiring the controls and accompanying representations written by Google as part of the Android operating systems ("Android OS") licensed to Android device manufacturers, such as Samsung.

5. Google's Privacy Policy also promised users control. That Privacy Policy states, on the first page:

> When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and ***put you in control***.
> . . . .
> Our ***services*** include: … ***products that are integrated into third-party apps*** and sites, like ads and embedded Google Maps.
> . . . .
> ***[A]cross our services, you can adjust your privacy settings to control what we collect and how your information is used***.

That language is quite plain. Any reasonable person would understand it to mean just what it says: the user "can adjust . . . privacy settings to control what [Google] collects and how [user] information is used" by Google "across [Google's] services," which services "include . . . products," like Google's Firebase SDK platform, "that are integrated into third-party apps."

6. In fact, Google still collects data from users who turn off the "Web & App Activity" feature. Google collects this data through various backdoors made available through and in connection with Google's Firebase Software Development Kit, including not only Google Analytics for Firebase but also without limitation [redacted]. All of these Firebase SDK products surreptitiously copy and provide Google with app activity data

while WAA is turned off, including personal browsing data.

7. Google accomplishes this surreptitious interception and collection using mobile devices to copy data from user communications with non-Google branded apps via and in connection with Google's Firebase SDK, including through background data collection processes such as Android's Google Mobile Service. Plaintiffs have requested but not yet received discovery from Google that is needed to understand the full scope of Google's unlawful data collection practices while WAA is turned off.

8. Google then uses the data it collects to create profiles and generate billions of dollars in revenues and other benefits. Google could have disclosed its collection and use of this data, while Web & App Activity is turned off, but Google chose not to. Instead, Google intentionally created an illusion of user control.

9. Because of its pervasive and unlawful interceptions of this data, Google knows users' friends, hobbies, political leanings, culinary preferences, cinematic tastes, shopping activity, preferred vacation destinations, romantic involvements, and even the most intimate and potentially embarrassing aspects of the user's app usage.

10. Google's practices affect millions of Americans who care about protecting their privacy. According to Google, more than 200 million people visit Google's "Privacy Checkup" website each year. Each day, nearly 20 million people check their Google privacy settings. People do this because they care about their privacy and believe that they can "control" what Google collects (because Google has told them so). The truth is that Google's so-called "controls" are meaningless. Nothing stops Google from collecting this data.

11. Google's practices unlawfully infringe upon consumers' privacy rights, give Google and its employees power to learn intimate details about individuals' lives, and make Google a potential target for "one-stop shopping" by any government, private, or criminal actor who wants to invade individuals' privacy.

12. Google must be held accountable for the harm it has caused. Google must be prevented from continuing to engage in its covert data collection from the mobile devices now in use by nearly every American citizen. Both federal and state privacy laws recognize and protect

individuals' reasonable expectations of privacy in confidential communications under these circumstances, and these laws prohibit Google's unauthorized interception and subsequent use of these communications.

13. Plaintiffs are individuals whose mobile devices transmitted data to Google as a result of Google's Firebase SDK scripts even though Plaintiffs had turned off the "Web and App Activity" feature. Plaintiffs bring California state law claims on behalf of other similarly situated Google subscribers in the United States (the "Classes," defined herein in paragraph 226). The Class Period begins on the date Google first received data, as a result of a Firebase SDK script, from the device of a user who had turned off the "Web & App Activity" feature. The Class Period continues through the present.

THE PARTIES

14. Plaintiff JulieAnna Muniz is an adult domiciled in El Cerrito, California. She had an active Google account during the Class Period.

15. Plaintiff Anibal Rodriguez is an adult domiciled in Homestead, Florida. He had active Google accounts during the Class Period.

16. Plaintiff Eliza Cambay is an adult domiciled in Torrance, California. She had active Google accounts during the Class Period.

17. Plaintiff Sal Cataldo is an adult domiciled in Sayville, New York. He had active Google accounts during the Class Period.

18. Plaintiff Emir Goenaga is an adult domiciled in Homestead, Florida. He had an active Google account during the Class Period.

19. Plaintiff Julian Santiago is an adult domiciled in Miami, Florida. He had an active Google account during the Class Period.

20. Plaintiff Harold Nyanjom is an adult domiciled in Wichita, Kansas. He had active Google accounts during the Class Period.

21. Plaintiff Kellie Nyanjom is an adult domiciled in Wichita, Kansas. She had active Google accounts during the Class Period.

22. Plaintiff Susan Lynn Harvey is an adult domiciled in Madera, California. She had

active Google accounts during the Class Period.

23. Defendant Google LLC is a Delaware limited liability company with a principal place of business at what is officially known as The Googleplex, 1600 Amphitheatre Parkway, Mountain View, California 94043. Google LLC regularly conducts business throughout California and in this judicial district. Google LLC is one of the largest technology companies in the world and conducts product development, search, and advertising operations in this district.

JURISDICTION AND VENUE

24. This Court has personal jurisdiction over Defendant because Google's principal place of business is in California. Additionally, Defendant is subject to specific personal jurisdiction in this State because a substantial part of the events and conduct giving rise to Plaintiffs' and Class members' claims occurred in this State, including Google servers in California receiving the intercepted communications and data at issue, and because of how employees of Google in California reuse the communications and data collected.

25. This Court has subject matter jurisdiction over this entire action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action in which the amount in controversy exceeds $5,000,000, and at least one Class member is a citizen of a state other than California or Delaware.

26. Venue is proper in this District because a substantial portion of the events and actions giving rise to the claims in this matter took place in this judicial District. Furthermore, Google is headquartered in this District and subject to personal jurisdiction in this District.

27. Intradistrict Assignment. A substantial part of the events and conduct which give rise to the claims herein occurred in Santa Clara County.

FACTUAL ALLEGATIONS REGARDING GOOGLE

I. Google Has a Long History of Invading Consumers' Privacy and Misrepresenting the Scope of Google's Data Collections

28. For at least the last decade, Google has been persistently and pervasively violating consumers' privacy rights. The pattern is always the same. Google gets caught. Google gets punished. Google lulls consumers into a false sense of security again.

29. In 2010, the FTC charged that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched its social network, Google Buzz." To resolve these claims, Google, in 2011, agreed to the FTC's entry of a binding Order (the "Consent Order"), which barred Google "from future privacy misrepresentations" and required Google "to implement a comprehensive privacy program."[2] The Consent Order also required Google to take steps relating to "covered information," defined as "information [Google] collects from or about an individual."[3] The FTC ordered as follows:

> **I.**
>
> **IT IS ORDERED** that [Google], in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:
>
> A. the extent to which [Google] maintains and protects the privacy and confidentiality of any covered information, including, but not limited to, misrepresentations related to: (1) the purposes for which it collects and uses covered information, and (2) the extent to which consumers may exercise control over the collection, use, or disclosure of covered information…[4]
>
> **II.**
>
> **IT IS FURTHER ORDERED** that [Google], prior to any new or additional sharing by respondent of the Google user's identified information with any third party, that: 1) is a change from stated sharing practices in effect at the time respondent collected such information, and 2) results from any change, addition, or enhancement to a product or service by respondent, in or affecting commerce, shall:
>
> A. Separate and apart from any final "end user license agreement," "privacy policy," "terms of use" page, or similar document, clearly and prominently disclose: (1) that the Google user's information

---

[2] *FTC Charges Deceptive Privacy Practices in Googles Rollout of Its Buzz Social Network*, FED. TRADE COMM'N (Mar. 30, 2011), https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz (last visited Nov. 11, 2020).

[3] The term "covered information" thus includes, but is not limited to, "(c) online contact information, such as a user identifier . . . (d) persistent identifier, such as IP address . . . (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above."

[4] Agreement Containing Consent Order, *In re Google Inc.*, No. 1023136 (F.T.C.), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf (emphasis added).

> will be disclosed to one or more third parties, (2) the identity or specific categories of such third parties, and (3) the purpose(s) for respondent's sharing; and
>
> B. Obtain express affirmative consent from the Google user to such sharing.

30. Google quickly recidivated. Just one year after entry of the Consent Order, the FTC found that Google had already violated it. In an August 2012 press release, the FTC explained that Google had been promising users of Apple's Safari web browser that Google would not track their web browsing, and that Google had then broken those promises by "circumventing the Safari browser's default cookie-blocking setting":

> Google Inc. has agreed to pay a record $22.5 million civil penalty to settle Federal Trade Commission charges that it misrepresented to users of Apple Inc.'s Safari Internet browser that it would not place tracking "cookies" or serve targeted ads to those users, violating an earlier privacy settlement between the company and the FTC.
>
> The settlement is part of the FTC's ongoing efforts make sure companies live up to the privacy promises they make to consumers, and is the largest penalty the agency has ever obtained for a violation of a Commission order. In addition to the civil penalty, the order also requires Google to disable all the tracking cookies it had said it would not place on consumers' computers.
>
> "The record setting penalty in this matter sends a clear message to all companies under an FTC privacy order," said Jon Leibowitz, Chairman of the FTC. "No matter how big or small, all companies must abide by FTC orders against them and keep their privacy promises to consumers, or they will end up paying many times what it would have cost to comply in the first place."[5]

31. Since 2012, a number of federal, state, and international regulators have similarly accused Google of violating its data-collection and privacy promises, with Google failing to disclose and obtain consent for its conduct.

---

[5] *Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FED. TRADE COMM'N (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented (last visited Nov. 11, 2020).

32. In January 2019, France's data privacy authority, known as the CNIL, fined Google $57 million for privacy violations. The violations related to: Google's lack of transparency regarding its data collection practices; Google's lack of valid consent from consumers; and the failure of Google's privacy settings to enable consumers to exercise real control over what Google collected.[6] In June 2020, France's highest court upheld this $57 million fine against Google, noting Google's failure to provide clear notice and obtain users' valid consent to process their personal data for ad personalization purposes on the Android mobile operating system. Google responded by stating that it had "'invested in industry-leading tools' to help its users 'understand and control how their data is used.'"[7]

33. In September 2019, Google and its YouTube subsidiary agreed to pay $170 million to settle allegations by the FTC and the New York Attorney General that YouTube illegally collected personal information from children without their parents' consent.[8]

34. There are ongoing proceedings by the Arizona Attorney General and the Australian Competition and Consumer Commission alleging that Google failed to obtain consent regarding its collection of location data and regarding its practices of combining certain user data.

35. In the Arizona Attorney General action, Google has produced documents establishing "overwhelming" evidence that "Google has known that the user experience they designed misleads and deceives users." Google's employees made numerous admissions in internal communications, recognizing that Google's privacy disclosures are a "mess" with regards to obtaining "consent" for its data-collection practices and other issues relevant in this lawsuit. Some of these documents were made publicly available on August 21, 2020 (ironically, with heavy privacy redactions by Google).

---

[6] Tony Romm, *France Fines Google $57 Million Under New EU Data-Privacy Law*, LOS ANGELES TIMES (Jan. 21, 2019), https://www.latimes.com/business/technology/la-fi-tn-google-france-data-privacy-20190121-story.html (last visited Nov. 11, 2020) (repost).

[7] The Associated Press, *Google Loses Appeal Against $56 Million Fine in France*, ABC NEWS (June 19, 2020), https://abcnews.go.com/Business/wireStory/google-loses-appeal-56-million-fine-france-71347227 (last visited Nov. 11, 2020).

[8] *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, FED. TRADE COMM'N (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations (last visited Nov. 11, 2020).

36. Some of the documents produced by Google in the Arizona Attorney General action refer to Google's "Web & App Activity" feature by name. These documents indicate that Google has long known that Google's disclosures about this feature were (at a minimum) highly confusing and insufficient to allow consumers to give informed consent. *See infra*, ¶¶ 78–79.

37. In an ongoing Australia proceeding, the Australian Competition & Consumer Commission ("ACCC") alleges that "Google misled Australian consumers to obtain their consent to expand the scope of personal information that Google could collect and combine about consumers' internet activity, for use by Google, including for targeted advertising." The ACCC alleges that Google impermissibly combined the data it collected directly from consumers with data that it received from "third-party sites and apps not owned by Google." The ACCC contends that Google "misled Australian consumers about what it planned to do with large amounts of their personal information, including internet activity on websites not connected to Google."[9]

II. Google Uses Firebase SDK to Surreptitiously Collect Users' Communications with Third-Party Apps

38. Mobile "apps" (shorthand for "applications") are software programs that run on mobile devices (e.g., smart phones, tablets).

39. Throughout the Class Period, the overwhelming majority of apps running on Class members' mobile devices have been third-party apps, meaning apps designed, developed, coded, and released by third-party developers. Google did not own or directly control these third-party developers.

40. Firebase SDK is a suite of software development tools that Google has owned and maintained throughout the Class Period. Firebase SDK is intended for use by third-party software developers, including developers of third-party apps for mobile devices. SDK stands for "software development kit." Google calls Firebase SDK a "comprehensive app development platform."

---

[9] *Correction: ACCC Alleges Google Misled Consumers About Expanded Use of Personal Data*, AUSTRALIAN COMPETITION & CONSUMER COMM'N (July 27, 2020), https://www.accc.gov.au/media-release/correction-accc-alleges-google-misled-consumers-about-expanded-use-of-personal-data#:~:text=The%20ACCC%20has%20launched%20Federal,Google%2C%20including%20for%20targeted%20advertising (last visited Nov. 11, 2020).

Google states that Firebase SDK allows developers to "build apps fast, without managing infrastructure," and that it is "one platform, with products that work better together."[10]

41. On May 20, 2016, Jason Titus, Vice President of Google's Developer Products Group, stated that more than 450,000 software developers were using Firebase SDK.

42. Throughout the Class Period, Google made significant efforts to coerce app developers to use Firebase SDK. For example:

a. Google requires third-party developers to use Firebase SDK in order to use the Google Analytics service to gain information about customers' use of the app;[11]

b. Google requires third-party developers to use Firebase SDK in order to make the app pages searchable on Android devices;

d. Google through Firebase SDK provides support for Google's "Play Store"—a platform on which third-party app developers distribute their app to consumers and process payments in the app.

43. As a result of Google's coercive practices, more than 1.5 million apps currently use Firebase SDK. That includes the vast majority of third-party apps that are currently in use on mobile devices that run Google's Android operating system. The third-party apps utilizing Firebase SDK include, for example, The New York Times, Duolingo, Alibaba, Lyft, Venmo, and The Economist.[12]

44. The Firebase SDK scripts copy and transmit to Google's servers in California many different kinds of user communications between app users on the one hand and, on the other hand, the app and the persons and entities who maintain the app (typically, the app's owners and developers), by overriding device and account level controls.

---

[10] *See* FIREBASE, https://firebase.google.com/ (last visited Nov. 11, 2020).

[11] For Android, see *Mobile App Reporting in Google Analytics - Android*, GOOGLE ANALYTICS, https://developers.google.com/analytics/devguides/collection/firebase/android (last visited Nov. 11, 2020) ("App reporting in Google Analytics is natively integrated with Firebase, Google's app developer platform . . . ."). For Apple iOS, see *Mobile App Reporting in Google Analytics - iOS*, GOOGLE ANALYTICS, https://developers.google.com/analytics/devguides/collection/firebase/ios (last visited Nov. 11, 2020) (also stating that "[a]pp reporting in Google Analytics is natively integrated with Firebase, Google's app developer platform . . . .").

[12] FIREBASE, https://firebase.google.com/ (last visited Nov. 11, 2020).

45. All of these communications qualify as "covered information" for purposes of the 2011 FTC Consent Order, and these communications contain personally identifiable information. These communications contain information relating to: (1) who the user is; (2) where the user is physically located; (3) what content the user has requested from the app (e.g., the app page URL); (4) what content the user has viewed on the app; and (5) much other information relating to the user's interaction with the app.

46. The Firebase SDK scripts cause the device to intercept these communications and send surreptitious copies of them to Google even if the user is not engaged with any Google site or functionality; even if the user is not logged in to his or her Google account; and even if the user has "turned off" the "Web & App Activity" feature. From the apps, the Firebase SDK then overrides the mobile device level controls, and causes the device to transmit the intercepted browsing data. Importantly, Google cannot receive this data without overriding device level settings, because the devices ultimately transmit and receive data, sitting between the user using the app, and the app server in the mobile cloud.

47. The Firebase SDK scripts do *not* cause the apps to give any notice to the user that the scripts are surreptitiously copying the communications and sending those copies to Google.

48. These Firebase SDK scripts work on all mobile devices running all the major operating systems—not just the Android system, but also Apple's iOS and many others. Specifically on Android OS, Google surreptitiously collects the app-browsing data through the Android GMS process, overriding device level controls.

49. To take just one example of the kind of communication that the Firebase SDK scripts intercept, secretly copy, and transmit to Google, even when the user has exercised their privacy controls: When a user selects a link to an article within The New York Times app on the user's phone, that selection generates a communication from the users' phone to The New York Times' servers. The New York Times' servers respond to the communication by transmitting data to the user's phone—the article, which then appears in the app. For users that have elected to not allow Google to track their app-browsing activity via their privacy controls, without disclosure or consent, Google (by means of the Firebase SDK scripts) intercepts the app user's request for that

content, surreptitiously copies the request, and then while overriding device and account level controls simultaneously transmits the browsing data to Google servers in California, where it is compiled with other data Google has collected and stored about that user. The interception and collection process runs vice versa as well, such as when the user is communicating back to the app publisher's server request via his or her mobile device.

50. Google's own documentation states that the Firebase SDK scripts allow Google to "[l]og the user's interactions with the app, including viewing content, creating new content, or sharing content."[13] The Firebase SDK scripts also allow Google to identify certain "actions" that consumers take within an app, such as "viewing a recipe." Thus, for example, Google's Firebase documentation states that Firebase can "log separate calls" each time a consumer "view[s] a recipe (start) and then clos[es] the recipe (end)." (This Google documentation, however, does *not* disclose that these scripts transmit this information and surreptitious copies of the data to Google even when the user switches the "Web & App Activity" feature off. And the documentation certainly does not disclose that Firebase SDK would be used to circumvent device and account level settings.)

51. Firebase SDK uses the term "event" to describe a wide range of user activity with an app. For example: when the user views a new screen on the app, that event is called "screen_view."[14] When the user opens a notification sent via the app from the Firebase Cloud Messaging system, that event is called "notification_open." And when the user selects content in the app, that event is called "select_content."

52. The Firebase SDK scripts "automatically" copy and transmit (to Google) communications relating to at least 26 different kinds of events (including "screen_view" and

---

[13] *Log User Actions*, FIREBASE, https://firebase.google.com/docs/app-indexing/android/log-actions (last visited Nov. 11, 2020). [redacted]

[14] *See Automatically Collected Events*, FIREBASE HELP, https://support.google.com/firebase/answer/6317485?hl=en#:~:text=Automatically%20collected%20events%20%20%20%20Event%20name,currency%2C%20quan%20...%20%2023%20more%20rows%20 (last visited Nov. 11, 2020).

"notification_open," described above), through the users' device. The Firebase SDK scripts will "collect" these events "automatically," meaning, even if the developer does not "write any additional code to collect these events."

53. In addition to the 26 different "automatically collected events," Firebase SDK permits app developers to code their apps to collect information about many more events (including "screen_view," described above). Furthermore, Firebase SDK enables developers to create their own "custom events" to be tracked in their apps.[15] Depending on how the app's code is written, Firebase SDK may also copy and transmit these and many additional events to Google's servers, through the users' device.

54. On Android OS, these intercepted messages are concurrently aggregated and facilitated by a background process called Google Mobile Service (GMS), which aggregates similarly intercepted messages across all the apps using Firebase SDK, so that user identity can be easily tracked across the apps, and so that browsing activity can be immediately associated and correlated for meaningful real-time context.

55. Firebase SDK associates almost every kind of event with one or more specific pieces of information, called "parameters." For example: when the user views a new screen (event: "screen_view"), the Firebase SDK scripts copy and transmit through the device at least seven different parameters to Google including "firebase_screen_id" and "engagement_time_msec." When the user opens a notification (event: "notification_open"), then the Firebase SDK scripts copy and transmit at least seven parameters to Google including "message_name," "message_time," "message_id," "topic," and "label." And when the user selects content in the app (event: "select_content"), then the Firebase SDK scripts copy and transmits through the device at least two parameters: "content_type" and "item_id."

56. The Firebase SDK scripts "automatically" copy and transmit five basic "parameters" about all events. These five automatically transmitted parameters are: "language";

---

[15] *Google Analytics 4 Properties Tag and Instrumentation Guide*, GOOGLE ANALYTICS, https://developers.google.com/analytics/devguides/collection/ga4/tag-guide (last visited Nov. 11, 2020).

"page_location"; "page_referrer"; "page_title"; and "screen_resolution."[16] According to Google, these five parameters are "collected by default with every event." This means that every time the user interacts with an app (in any sort of event), Firebase records that interaction by copying and transmitting to Google's servers through the device at least those five parameters.

57. Focusing just on the three of the five "parameters" that Google "automatically" transmits: the "page_title" parameter informs Google what the user is viewing; the "page_referrer" parameter informs Google whether the user arrived at that page from another place where Google has a tracker (and if so, the identity of that other place); and the "page_location" parameter informs Google of the URL address (e.g., internet address) of the content the user is viewing on his or her device.

58. Google does not notify its users of these Firebase SDK scripts and how Google actually uses them, which cause the copying and duplication of browsing data to be sent to Google, for at least Google Analytics for Firebase, [redacted]. These scripts are hidden from users and run without any notice to users of the interception and data collection even when they exercise their device level controls, which exceeds all contemplated and authorized use of the users' data. All of these Firebase SDK products surreptitiously provide app browsing data to Google on mobile devices, overriding their device level controls, including through background processes such as Android GMS.

59. Users have no way to remove these Firebase SDK scripts or to opt-out of this data collection. Google intentionally designed these scripts in such a way as to render ineffective any barriers users may attempt to use to prevent access to their information, including by turning off the "Web & App Activity" feature.

[16] *Automatically Collected Events*, FIREBASE HELP, https://support.google.com/firebase/answer/6317485?hl=en#:~:text=Automatically%20collected%20events%20%20%20%20Event%20name,currency%2C%20quan%20...%20%2023%20more%20rows%20 (last visited Nov. 11, 2020).

III. Users Turned off the "Web & App Activity" Feature to Prevent Google from Collecting Users' Communications with Third-Party Apps, but Google Continued Without Disclosure or Consent to Intercept Those Communications

A. Google's "Web & App Activity" Feature

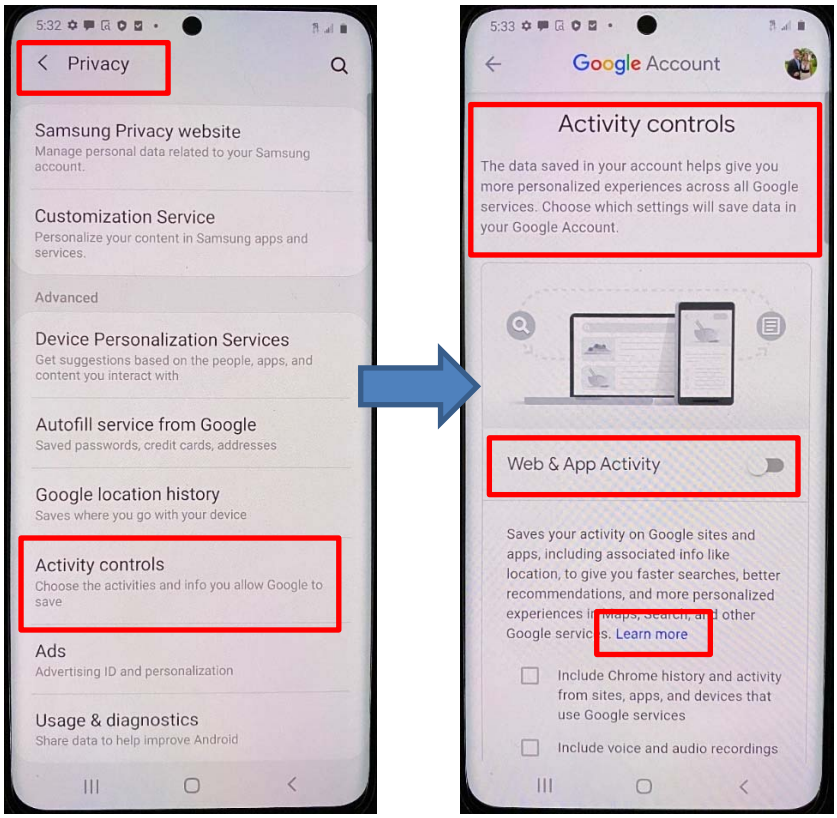
60. In or before 2015, Google launched the "Web & App Activity" feature.

61. Throughout the Class Period, users have been able to access the Web & App Activity feature in at least two ways: through Google's website, and through the "Settings" menu of a mobile device running Android OS. Google presented such settings to their business partners as device level controls, including by requiring the controls and accompanying representations written by Google as part of the Android OS, as licensed to Android device manufacturers, such as Samsung.

62. To access the "Web & Activity" feature through Google's website, a user would direct his or her web browser to Google's My Activity website (and previously Google's My Account website), and would then log on with their Google account credentials. The first screen of the My Activity website displays, among other options, the "Web & App Activity" feature. By clicking on the words "Web & App Activity," the user is taken to a second screen, which displays the image of a switch beside the words "Web & App Activity." The user can then toggle the switch "off" to turn off the "Web & App Activity" feature.[17]

63. To access the "Web & Activity" feature through a mobile device running Google's Android operating system, the user would use the phone's "Settings" application. For example, on a Samsung phone running the Android system, the "Settings" application includes a section entitled "Privacy Controls." (Shown in "Screen 1," below.) Within that "Privacy Controls" menu, the user can select "Activity Controls," which would open a new screen. (Shown in "Screen 2," below.) In that second "Activity Controls" screen, the phone displays the image of a switch beside the words "Web & App Activity." The user can then toggle the switch "off" to turn off the "Web & App Activity" feature.

[17] Google previously offered the option to "pause" Web & App Activity. "Pausing" this feature likewise did not stop the Google interception, data collection, and use at issue in this lawsuit.



SCREEN 1[18] SCREEN 2

64. Google simultaneously tracks the user's setting of the "Web & App Activity" feature (whether "on" or "off") across all Google's services and devices in real time. Thus, if a user turns off "Web & App Activity" in the user's phone, then that change will also be reflected when the user logs on to Google's "My Activity" website using the user's laptop. Similarly, if a user then uses the laptop to turn "Web & App Activity" back "on," using the "My Activity" website, then this feature will also be turned "on" in the user's Android phone "Settings" application.

65. However, contrary to Google's disclosures (described below), turning off the "Web & App Activity" feature actually does nothing to stop Google from receiving, collecting, and using the data transmitted to Google by the Firebase SDK scripts. Those surreptitious transmissions are, without disclosure or consent, unaffected by the "Web & App Activity" feature.

[18] The highlighted language from this screen is part of the OS language written by Google.

B. Google's Privacy Policy and "Learn More" Disclosures Stated That the "Web & App Activity" Feature Stops Google from "Saving" Users' Data

66. Throughout the Class Period, Google stated that turning "off" the "Web & App Activity" feature would prevent Google from collecting users' app activity, including users' communications made via apps. Google's statements appeared in at least three places: Google's "Privacy Policy"; Google's "Privacy and Security Principles"; and Google's "Learn More" disclosures relating to the "Web & App Activity" feature.

1. Google's "Privacy Policy" and "Privacy and Security Principles" Stated That Users Could "Control" What Google Collects

67. Throughout the Class Period, Google's Privacy Policy has defined "Google services" to include Google products that, like Firebase SDK, are "integrated into third-party apps." The first page of Google's Privacy Policy states:

> Our ***services include:*** . . . ***Products that are integrated into third-party apps*** and sites, like ads and embedded Google Maps

Ex. A at 1 (Privacy Policy).

68. From at least May 25, 2018, to the present, Google's Privacy Policy has promised users that "***across our services***, ***you*** can adjust your privacy settings to ***control what we collect and how your information is used***." *Id.* (emphasis added).[19] Earlier versions of Google's Privacy Policy included similar representations.[20]

---

[19] *See* Privacy Policy, GOOGLE PRIVACY & TERMS, https://policies.google.com/privacy (last visited Nov. 11, 2020). Google included this same statement—"you can adjust your privacy settings to control what we collect and how your information is used"—in versions of its Privacy Policy dated May 25, 2018, January 22, 2019, October 15, 2019, December 19, 2019, March 31, 2020, July 1, 2020, August 28, 2020, and September 30, 2020. *Id.*

[20] The Google Privacy Policies effective between August 19, 2015 and May 24, 2018 included a section titled "Transparency and choice." That section states that Google's "goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used" and directs users to "[r]eview and update your Google activity controls to decide what types of data, such as videos you've watched on YouTube or past searches, you would like saved with your account when you use Google services." Also included in the "Transparency and choice" section is the statement that users can "[c]ontrol who you share information with through your Google Account." *See* Aug. 19, 2015 Google Privacy Policy; Mar. 25, 2016 Google Privacy Policy; June 28, 2016 Google Privacy Policy; Aug. 29, 2016 Google Privacy Policy; Mar. 1, 2017 Google Privacy Policy; Apr. 17, 2017 Google Privacy Policy; Oct. 2, 2017 Google Privacy Policy; Dec. 18, 2017 Google Privacy Policy (this policy was effective until May 24, 2018).

69. Throughout the Class Period, Google's Privacy Policy has told users that they can "control data" by using Google's "My Activity" website. (As described above, "My Activity" is the website that users can access in order to switch "Web & App Activity" off.) The Privacy Policy states: "My Activity allows ***you to*** review and ***control data that's created when you use Google services*** . . . ." Ex. A at 9 (Privacy Policy) (emphasis added).

70. Google also stated in its "Privacy and Security Principles," displayed on its "Safety Center" website,[21] that Google would: "[r]espect our users" and "their privacy"; "[b]e clear about what data we collect"; "make it easy to understand what data we collect"; and "[m]ake it easy for people to control their privacy." Google further stated, in these Privacy and Security Principles: "Every Google Account is built with on/off data controls, so our users can choose the privacy settings that are right for them." Google promised to "ensur[e] that privacy is always an individual choice that belongs to the user." These "principles" have been part of Google's successful efforts to lull users, app developers, and others into a false sense of user control and privacy.

2. Google's "Learn More" Disclosures with Respect to "Web & App Activity" Explained That Turning the Feature off Would Prevent Google from Saving Information Related to Third Party Apps

71. As described above, Google's "My Activity" website is one of two ways users can switch off "Web & App Activity." That website contains a hyperlink with the words "Learn more," located below the on/off switch for "Web & App Activity." When users click on this "Learn more" hyperlink, their browser then displays a new webpage entitled "See & Control your Web & App Activity."[22] On that page, during the Class Period, Google made the following disclosures:

---

[21] *Our Privacy and Security Principles*, GOOGLE SAFETY CENTER, https://safety.google/principles/ (last visited Nov. 11, 2020).

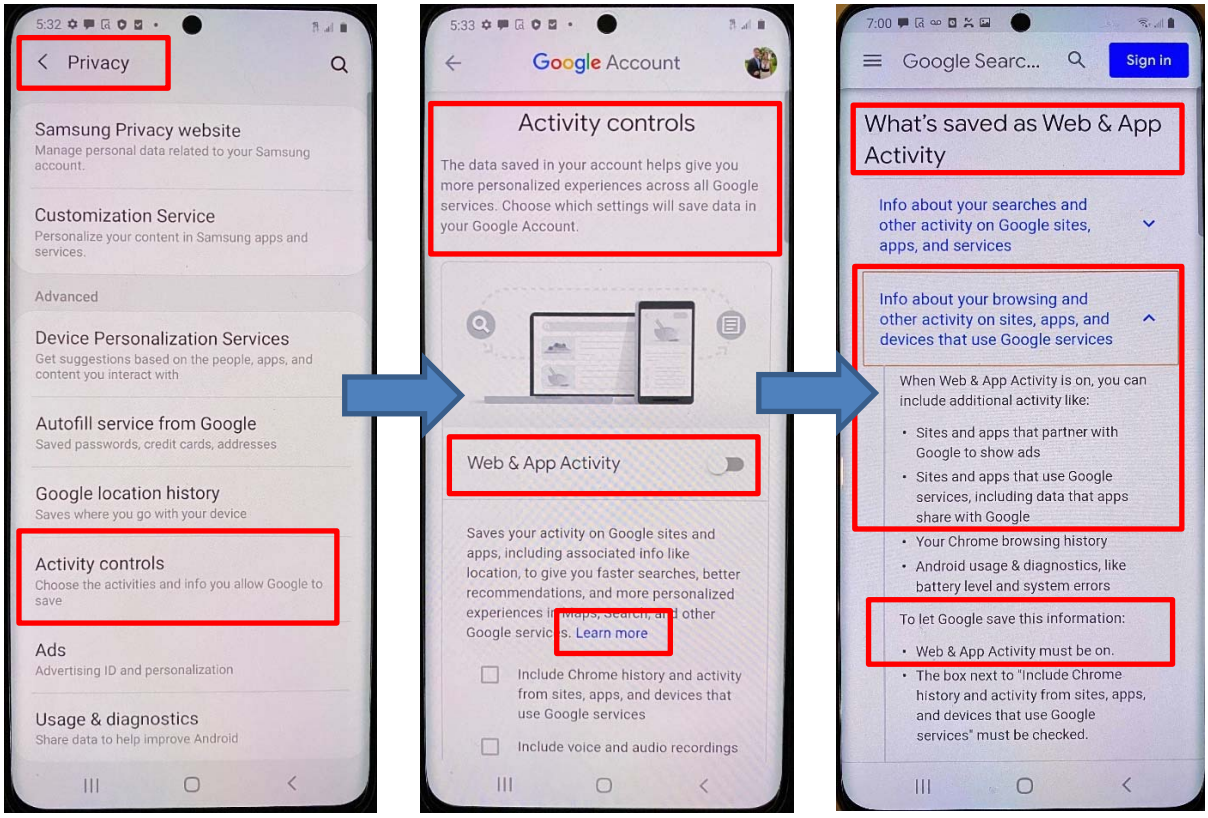
[22] *See & Control Your Web & App Activity*, GOOGLE SEARCH HELP, https://support.google.com/websearch/answer/54068?visit_id=637255508625725742210537612 8&hl=en&rd=1 (last visited Nov. 11, 2020).

> **SEE & CONTROL YOUR WEB & APP ACTIVITY**
>
> . . . .
>
> You can turn Web & App Activity off or delete past activity at any time…
>
> **I. What's saved as Web & App Activity…**
>
> Info about your browsing and other activity on sites, apps, and devices that use Google services
>
> When Web & App Activity is on, you can include additional activity like:
>
> - Sites and apps that partner with Google to show ads
> - Sites and apps that use Google services, including data that apps share with Google
> - Your Chrome browsing history
> - Android usage & diagnostics, like battery level and system errors
>
> ***To let Google save this information:***
>
> - ***Web & App Activity must be on***.
> - The box next to "Include Chrome history and activity from sites, apps, and devices that use Google services" must be checked.

Id. (emphases added). This is a plain and direct statement to users that the switch for "Web & App Activity" "must be on" "[t]o let Google save this information," including "[i]nfo about" the users' "activity on sites, apps, and devices that use Google services." *Id.* "Google services" includes, of course, Firebase SDK, and hundreds of thousands of apps use this "service." Google's own Privacy Policy defines the term "Google service" to include Firebase SDK. Ex. A at 1 (Privacy Policy) ("Our ***services include:*** . . . ***products that are integrated into third-party apps*** . . . .").

72. Google's "Learn More" disclosures on the Android "settings" screens also stated that turning the Web & App Activity feature off would prevent Google from "sav[ing]" information related to third-party apps. As described above, users with devices running Google's Android operating system have an additional means of switching the "Web & App Activity" feature off—namely, they can do this using the "Activity Controls" section of the "Privacy" menu within these devices' "Settings" application. *Supra*, ¶ 63. This section also contains a "Learn more" hyperlink (see bottom of Screen 2, below) which, if selected, opens a web browser application on the device and displays to the user the same webpage, entitled "See & Control your Web & App Activity," within Google's "My Activity" website. *Supra*, ¶ 71 (describing and

quoting this webpage). (Screen 3, below, shows a screenshot of part of this webpage as displayed on the device.)



SCREEN 1 SCREEN 2 SCREEN 3

73. In Screen 1, the user is promised that the "Activity controls" will enable the user to "[c]hoose the activities and info you allow Google to save."

74. In Screen 3, after selecting "Learn more," the user is told that "To let Google save this information: Web & App Activity must be on."

75. Thus, users who used their Android "Settings" application to learn more about the "Web & App Activity" feature received the same misleading disclosures as did users who visited the "My Activity" website.

76. Based on Google's disclosures described and quoted above, Plaintiffs and Class members had the objectively reasonable belief that Google would stop collecting their communications and other interactions with apps on their phones—"across [Google's] services"—if the users turned the "Web & App Activity" switch to "off."

77. Plaintiffs and Class members could not possibly have consented to Google's collection of their communications and other interactions with apps on their mobile devices when they turned the "Web & App Activity" switch to off.

3. Google Knew That Its Disclosures Led Users to Believe That Turning "Web & App Activity" off Would Prevent Google from Collecting Communications with Apps

78. As a result of the Arizona Attorney General's ongoing investigation (*see supra*, ¶¶ 34–36), several heavily redacted internal Google documents have been made public. These documents refer to Google's "Web & App Activity" feature and its on/off switch. The documents indicate that Google's own employees understood that Google's disclosures to consumers, regarding this switch, misled consumers into believing, wrongly, that turning the switch "off" would prevent Firebase SDK from transmitting users' communications to Google. For example:

a. On February 2, 2017, one Google employee (name redacted by Google for privacy reasons) referenced "work in progress" at Google "trying to rein in the overall mess that we have with regards to data collection, consent, and storage." This was in response to another Google employee (name redacted by Google for privacy reasons), asking a question regarding whether "users with significant privacy concerns understand what data we are saving?" Another Google employee (name redacted by Google for privacy reasons) stated that this area was "super messy" and users needed to "make sense out of this mess." The "overall mess" with Google's data collection and consent described in these documents includes the Web & App Activity feature.

b. On August 13, 2018, one Google employee (name redacted by Google for privacy reasons) referenced "Web/App Activity" and commented that the "current UI [user interface] feels like it is designed to make things possible, yet difficult enough that people won't figure it out." The Google employee also noted that selections were "defaulted to on, silently appearing in setting menus you may never see is <redacted>." These internal Google comments specifically addressed Web & App Activity, characterizing Web & App Activity as something "difficult enough" that users "won't figure it out."

c. On August 14, 2018, one Google employee (name redacted by Google for

privacy reasons) referenced Web & App Activity, stating "I did not know Web and App activity had anything to do with location. And seems like we are not good at explaining this to users." Another Google employee (name redacted by Google for privacy reasons) added: "Definitely confusing from a user point of view if we need googlers [to] explain it to us[.]" Google employees recognized Google was "not good" (perhaps intentionally so) at explaining the Web & App Activity feature.

d. One heavily redacted 2017 Google presentation concerns a study that specifically focused, at least in part, on "Consent" and asked, "Do users comprehend what will happen if they turn on the Web & App activity setting . . . ." The presentation includes a lengthy, but mostly redacted, section of "Detailed findings." Those findings state that "Participants had difficulty [redacted]" and that the "effect of the activity of the Web & App Activity [redacted]."

79. On information and belief, unredacted versions of those documents and other internal Google documents will further confirm that not even Google believes its users had consented to Google's interceptions between users and apps when "Web & App Activity" was switched off.

4. Google's Passing Reference to "Your Google Account" Does Not Constitute Consent

80. During the Class Period, Google made much of its commitment to privacy. For example, Google's CEO promised consumers, in a *New York Times* op-ed, that "[t]o make privacy real, we give you clear, meaningful choices around your data."[23]

81. Now faced with this lawsuit compelling it to honor these claims, Google has abandoned this commitment to clear and meaningful choices, instead contending that its Privacy Policy and promises were a ruse.

82. Google's first motion to dismiss contended—incorrectly and incredibly—that the "Learn more" disclosures described above somehow told users that Google would continue to intercept, copy, collect and save their communications with apps, even when the "Web & App

[23] Sundair Pichai, *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, THE NEW YORK TIMES (May 7, 2019), *available at* https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html (last visited Nov. 11, 2020).

Activity" feature was turned "off." Google's motion relied on the words "saved in your Google Account," taken from a single sentence in the "See & Control your Web & App Activity" page:

> If Web & App Activity is turned on, your searches and activity from other Google services are ***saved in your Google Account***, so you may get more personalized experiences, like faster searches and more helpful app and content recommendations.

Google argued that the words "saved in your Google Account" conveyed to users that the "Web & App Activity" on/off switch was meaningless—that it would not do precisely what Google's Privacy Policy (and the rest of the "Learn More" hyperlinked page) says that the switch would do. Rather, these five words, according to Google, indicate that the "off" switch has all the effect of a light switch during a blackout: The switch merely toggles off what data Google will *display for the user* in the user's "account." To state this contention plainly reveals how outlandish it is. Over and over again Google's Privacy Policy and "Learn more" disclosures told users that the "Web & App Activity" feature switch would "control" what "Google saves"; "what we collect"; and "how your information is used"—across "Google services." The five words highlighted by Google do nothing to diminish Google's promises.

83. Google's reliance on these five words is particularly weak because Google itself, in many other disclosures, told users that Google promised to "Be clear about what data we collect and why. To help people make informed decisions about how they use Google products, we make it easy to understand what data we collect, how it's used, and why. Being transparent means making this information readily available, understandable, and actionable."[24] *See infra*, ¶¶ 86–104 (collecting such public statements by Google). Google's made-for-litigation argument, relying on a passing reference to "activity" being "saved in your Google account," is not the kind of "easy to understand" and "transparent" disclosure Google elsewhere promised to its users.

84. Google's argument is wrong for another reason, too: This sentence refers only to what happens if "Web & App Activity ***is turned on.***" Nothing in this sentence limits Google's repeated promises, quoted above, about what would happen when users turned Web & App

[24] *Our Privacy and Security Principles*, Google Safety Center, https://safety.google/principles/ (last visited Nov. 11, 2020).

Activity ***off***. Plaintiffs and the Class members were never told about and were harmed by Google's continued interceptions and collections of data during the times when they turned the switch ***off***.

85. Critically, nowhere in any disclosures did Google ever state that it would continue to collect users' communications with apps when the "Web & App Activity" feature was turned off. Because nothing in the Privacy Policies or other disclosures state that Google intercepts communications between users and apps when "Web & App Activity" is turned off, the notion that users and apps consented to this practice is absurd—one cannot consent to what one does not know.

C. Google Obscured Its Collection of These Communications Without Consent Through Its "Pro-Privacy" Campaigns and Other Public Statements

86. In addition to the Privacy Policy and "Learn More" disclosures, described above, Google masked its unauthorized data collection practices (including specifically Google's practice of receiving, collecting, and saving the Firebase SDK transmissions while users had switched off the "Web & App Activity" feature) through various "pro-privacy" campaigns and other public statements.

87. On June 1, 2015, Google Product Manager of Account Controls and Settings, Guemmy Kim, published an article titled "Keeping your personal information private and safe—and putting you in control."[25] The article states that "Google builds simple, powerful privacy and security tools that keep your information safe and put you in control of it," such as the "new hub" called "My Account" (which at that time included the Web & App Activity feature that is at issue in this lawsuit). This article told users that "My Account gives you quick access to the settings and tools that help you safeguard your data, protect your privacy, and decide what information is used to make Google services work better for you." The article stated that users can "[m]anage the information" that Google "use[s]" from Google "products." As an example of how users can control how Google uses their information, the article further represented that "you can turn on and off settings such as Web and App Activity."

[25] Guemmy Kim, *Keeping Your Personal Information Private and Safe—and Putting You in Control*, GOOGLE, THE KEYWORD (June 1, 2015), *available at* https://blog.google/topics/safety-security/privacy-security-tools-improvements/ (last visited Nov. 11, 2020).

88. On June 1, 2016, Kim published another article titled "Celebrating My Account's first birthday with improvements and new controls." This article described Google's My Account hub (which at that time included the Web & App Activity feature at issue in this lawsuit) as "a hub that gives you quick access to controls for safeguarding your data and protecting your privacy on Google."[26] The article touted how Google's tools "make it easy for you to control your privacy" and represented that when "you entrust your data to Google, you should expect powerful security and privacy controls."

89. On September 8, 2017, Google Product Manager Greg Fair published an article titled "Improving our privacy controls with a new Google Dashboard" in which he touted how Google has "[p]owerful privacy controls that work for you" and emphasized that users had "control" over their information and tools "for controlling your data across Google."[27] Mr. Fair specifically referenced the My Activity hub (formerly named "My Account"), which at that time included the Web & App Activity feature at issue in this lawsuit. Mr. Fair stated: "You–and only you–can view and control the information in My Activity." After describing this privacy control, Mr. Fair boasted Google's efforts in "[b]uilding tools that help people understand the data stored with their Google Account and control their privacy."

90. On June 21, 2018, Google Product Manager, Jon Hannemann, published an article titled "More transparency and control in your Google Account" in which he wrote: "For years, we've built and refined tools to help you easily understand, protect, and control your information. As needs around security and privacy evolve, we will continue to improve these important tools to help you control how Google works for you."[28]

---

[26] Guemmy Kim, *Celebrating My Account's First Birthday with Improvements and New Controls*, GOOGLE, THE KEYWORD (June 1, 2016), *available at* https://blog.google/technology/safety-security/celebrating-my-accounts-first-birthday/ (last visited Nov. 11, 2020).

[27] Greg Fair, *Improving Our Privacy Controls with a New Google Dashboard*, GOOGLE, THE KEYWORD (Sept. 8, 2017), https://www.blog.google/topics/safety-security/improving-our-privacy-controls-new-google-dashboard/ (last visited Nov. 11, 2020).

[28] Jan Hannemann, *More Transparency and Control in Your Google Account*, GOOGLE, THE KEYWORD (June 21, 2018), https://blog.google/technology/safety-security/more-transparency-and-control-your-google-account/ (last visited Nov. 11, 2020).

91. On May 7, 2019, Google CEO Pichai published an op-ed in the *New York Times*, titled "Privacy Should Not Be a Luxury Good," in which he stated that: "we [at Google] care just as much about the experience on low-cost phones in countries starting to come online as we do about the experience on high-end phones. Our mission compels us to take the same approach to privacy. For us, that means privacy cannot be a luxury good offered only to people who can afford to buy premium products and services."[29] Mr. Pichai further stated that it is "vital for companies to give people clear, individual choices around how their data is used" and that Google focuses on "features that make privacy a reality — for everyone." He continued: "To make privacy real, we give you clear, meaningful choices around your data."[30]

92. On the same date, May 7, 2019, Google CEO Pichai gave the keynote address at Google's 2019 I/O developer conference. He stated: "[a]nother way we build for everyone is by ensuring that our products are safe and private, and that people have clear, meaningful choices around their data. We strongly believe that privacy and security are for everyone, not just a few." The full text of his remarks was later published online.[31] Mr. Pichai further stated that Google's "products" are "built on a foundation of user trust and privacy." He represented that Google "ensur[es] that our products are safe and private, and that people have clear, meaningful choices around their data."[32] Recognizing that "privacy and security are for everyone," he also stated: "This is why powerful privacy features and controls have always been built into Google services." Mr. Pichai specifically referenced the Web & App Activity control at issue in this lawsuit, touting how Google was launching the auto-delete functionality as an example of how users can access "privacy controls" to "easily change your privacy settings."

---

[29] Sundar Pichai, *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, THE NEW YORK TIMES (May 7, 2020), *available at* https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html (last visited Nov. 11, 2020).

[30] *Id.*

[31] Pangambam S., *Sundar Pichai at Google I/O 2019 Keynote (Full Transcript)*, THE SINGJU POST (June 13, 2019), *available at* https://singjupost.com/sundar-pichai-at-google-i-o-2019-keynote-full-transcript/?singlepage=1.

[32] *Id.*

93. In August 2019 Google launched a "pro-privacy" campaign called "Privacy Sandbox." In this campaign, Google promotes itself as a champion of privacy and choice that scrupulously respects the privacy of its users and is transparent about the data it collects.[33] The blog post announcing this initiative declared to users that "Privacy is paramount to us, in everything we do."

94. Since the Privacy Sandbox campaign, Google has indicated that it will require rival adtech companies using Google targeted advertising products to have their own consent directly from the consumers, if the rival adtech companies are to track consumers directly. In response to questions from regulators—such as those in the United Kingdom—regarding whether Google was engaged in anticompetitive conduct, Google responded by indicating that it was protecting consumer privacy.

95. On October 2, 2019, Google Director of Product Management, Privacy, and Data Protection Office, Eric Miraglia, published an article titled "Keeping privacy and security simple, for you" in which he represented that when it comes to "privacy and security," "managing your data should be just as easy as making a restaurant reservation."[34] He emphasized how Google was "rolling out more ways for you to protect your data . . . ." He referenced Web & App Activity, stating that Google was allowing users to "automatically delete your Location History and Web & App Activity, which includes things you've searched for and browsed."

96. On December 19, 2019, Google Vice President of Product Privacy Rahul Roy-Chowdhury published an article titled "Putting you in control: our work in privacy this year" in which he represented that Google Account (which includes the Web & App Activity control at issue in this lawsuit) is a "tool[] for users to access, manage and delete their data" and that Google

---

[33] Justin Schuh, *Building a More Private Web*, Google, The Keyword (Aug. 22, 2019), *available at* https://www.blog.google/products/chrome/building-a-more-private-web/ (last visited Nov. 11, 2020).

[34] Eric Miraglia, *Keeping Privacy and Security Simple, For You*, GOOGLE, THE KEYWORD (Oct. 2, 2019), *available at* https://blog.google/technology/safety-security/keeping-privacy-and-security-simple-you/ (last visited Nov. 11, 2020).

"let[s] you control how your information is used."[35]

97. On January 22, 2020, Google CEO Pichai stated that privacy "cannot be a luxury good," and claimed that "privacy" is "at the heart of what we do."[36]

98. On January 28, 2020, Google Vice President of Product Privacy Rahul Roy-Chowdhury published an article titled "Data Privacy Day: seven ways we protect your privacy" in which he identified the Web & App Activity feature and explained how Google's auto-delete functionality would allow users to "choose to have Google automatically and continuously delete your activity and location history after 3 or 18 months. You can also control what data is saved to your account with easy on/off controls in your Google Account, and even delete your data by date, product and topic."[37]

99. On May 7, 2020, Google Director of Product Management, Privacy and Data Protection Office, Eric Miraglia published an article titled "Privacy that works for everyone" in which he wrote that "you should be able to understand and manage your data–and make privacy choices that are right for you."[38] He referenced the privacy features and controls at issue in this lawsuit, with Web & App Activity, and wrote: "A few years ago, we introduced Google Account to provide a comprehensive view of the information you've shared and saved with Google, and one place to access your privacy and security settings. Simple on/off controls let you decide which activity you want to save to your account" and you "can also choose which activities or categories of information you want to delete." He also touted the "new control" for "Web & App Activity" with the auto-deletion of "your Location History and Web & App Activity data.

---

[35] Rahul Roy-Chowdhury, *Putting You in Control: Our Work in Privacy This Year*, GOOGLE, THE KEYWORD (Dec. 19, 2019), *available at* https://blog.google/technology/safety-security/putting-you-in-control-privacy-2019/ (last visited Nov. 11, 2020).

[36] James Warrington, *Privacy "Cannot Be a Luxury Good," Says Google Boss Under Pichai*, CITY A.M. (Jan. 22, 2020), *available at* https://www.cityam.com/privacy-cannot-be-a-luxury-good-says-google-boss-sundar-pichai/ (last visited Nov. 11, 2020).

[37] Rahul Roy-Chowdhury, *Data Privacy Day: Seven Ways We Protect Your Privacy*, GOOGLE, THE KEYWORD (Jan. 28, 2020), *available at* https://blog.google/technology/safety-security/data-privacy-day-seven-ways-we-protect-your-privacy/ (last visited Nov. 11, 2020).

[38] Eric Miraglia, *Privacy That Works for Everyone*, GOOGLE, THE KEYWORD (May 7, 2019), *available at* https://blog.google/technology/safety-security/privacy-everyone-io/ (last visited Nov. 11, 2020).

100. On June 24, 2020, Google CEO Sundar Pichai published an article titled "Keeping your private information private" in which he represented that "[p]rivacy is at the heart of everything we do" and that Google focuses on "putting you in control" and "working to give you control on your terms."[39] Mr. Pichai specifically referenced Web & App Activity as part of those efforts to treat "your information responsibly" and stated that Google changed its default settings for "new accounts" so that "your activity data will be automatically and continuously deleted after 18 months, rather than kept until you choose to delete it."

101. On or about July 29, 2020, Google submitted written remarks to Congress for testimony by its current CEO Pichai (who helped develop Google's Chrome browser), which stated: "I've always believed that privacy is a universal right and should be available to everyone, and Google is committed to keeping your information safe, treating it responsibly, and putting you in control of what you choose to share."[40]

102. On September 15, 2020, Google's Global Partnership and Corporate Development President Donald Harrison stated during a Senate hearing that consent at times "appears confusing" but also represented that users "have control" and that Google wants "our users to be able to make a decision on how they control their data . . . ." He represented that "[u]sers own their data" and that users were "able to make a decision on how they control their data."

103. The statements by Google and its key leaders, described above, were widely publicized to Google users by many different news outlets, which correctly interpreted these statements as claims, by Google, to be safeguarding users' privacy.[41] Google intended these

---

[39] Sundar Pichai, *Keeping Your Private Information Private*, GOOGLE, THE KEYWORD (June 24, 2020), *available at* https://blog.google/technology/safety-security/keeping-private-information-private/ (last visited Nov. 11, 2020).

[40] *Online Platforms and Market Power, Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google: Hearing Before the Subcomm. on Antitrust, Commercial, and Administrative Law of the H. Comm. on the Judiciary*, July 29, 2020, https://docs.house.gov/meetings/JU/JU05/20200729/110883/HHRG-116-JU05-Wstate-PichaiS-20200729.pdf (written testimony of Sundar Pichai, Chief Executive Officer, Alphabet Inc.).

[41] Jon Porter, *Google's Sundar Pichai Snipes at Apple with Privacy Defense*, THE VERGE (May 8, 2019), *available at* https://www.theverge.com/2019/5/8/18536604/google-sundar-pichai-privacy-op-ed-nyt-regulation-apple-cook-advertising-targeting-user-data (last visited Nov. 11, 2020).

statements to communicate that Google's data-collection practices were more transparent, and more respectful of users' privacy, than were the practices of Google's competitors (e.g., Apple).

104. Google and its key leaders made the statements described above in order to obscure Google's intent to engage in widespread data collection without consent. These statements were intended to convey, and did convey, that Google did not intercept and collect users' data when the users had turned off the "Web & App Activity" feature.

D. Third-Party App Developers Did Not Consent to Google Collecting Users' Communications with Third-Party Apps When "Web & App Activity" Was Turned off

105. Third-party app developers who used Firebase SDK likewise did not consent to Google's interception of users' communications with apps when "Web & App Activity" was turned off. Throughout the Class Period, Google told these developers, in the service agreements, that Google: (1) would comply with its own Privacy Policy; (2) would provide app users with control over their data; and (3) would help the developers to comply with privacy laws and to protect consumers' rights over their data, such as consumers' rights to "access; rectification; restricted processing; [and] portability."

106. Google represented and continues to represent to app developers that Google will adhere to its own Privacy Policy. Specifically, Google states the following, on the Analytics Help page intended for use by app developers who use Firebase SDK:

//

//

//

//

//

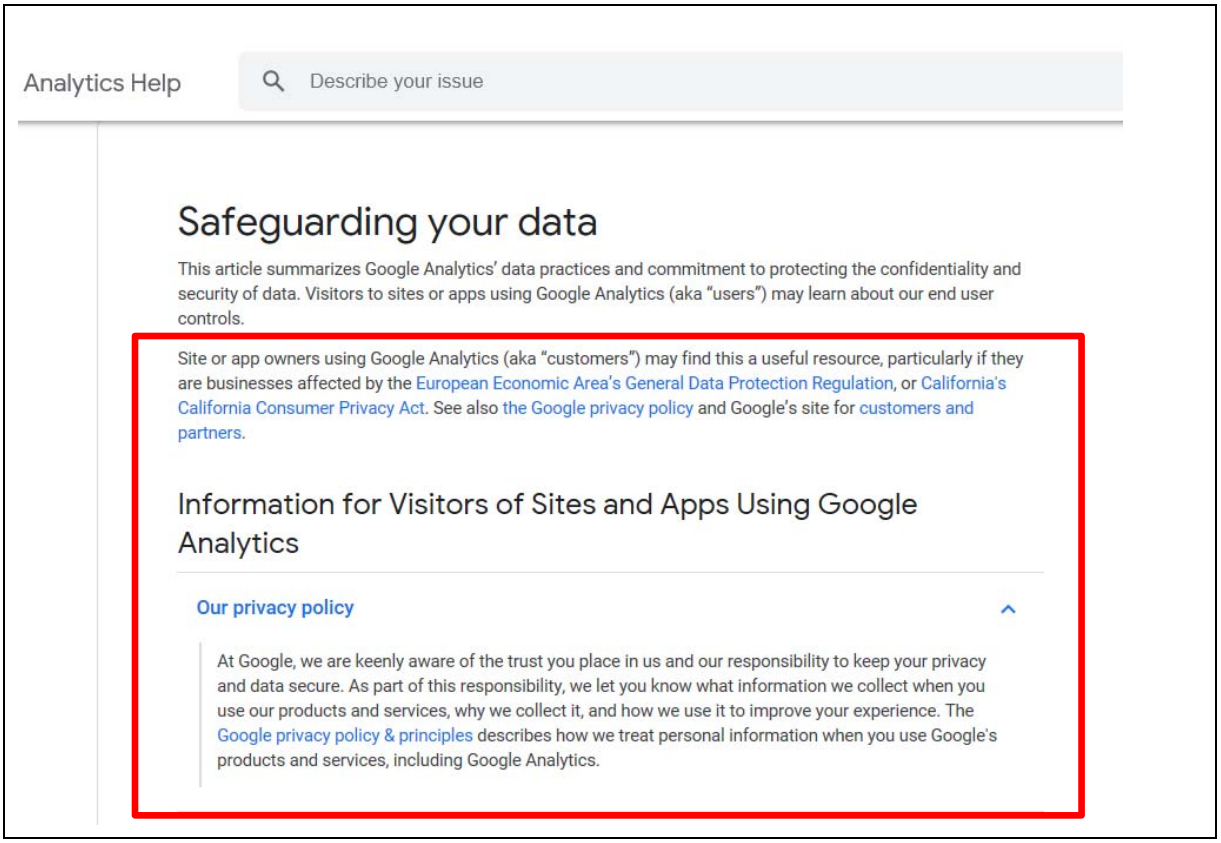
//

//

//

//

//



107. When any app developer clicks on the "Google privacy policy & principles" above, they are taken to Google's Privacy Policy page—the same Privacy Policy page described above. *Supra*, ¶¶ 67-69.[42] In its Privacy Policy, Google falsely stated to its users that "***across our services***, ***you*** [the user] can adjust your privacy settings to ***control what we collect and how your information is used***." As discussed above, Google's Privacy Policy also promises users that Google's "My Activity" website "allows you [the user] to review and control data that's created when you use Google services."

108. Google also gave and gives assurances to app developers in its "Firebase Data Processing And Security Terms" that Google "will protect users' privacy."[43] The purpose of these

[42] Google Privacy Policy, GOOGLE PRIVACY & TERMS, https://policies.google.com/privacy?hl=en.

[43] Firebase Data Processing and Security Terms, FIREBASE, https://firebase.google.com/terms/data-processing-terms#9.-data-subject-rights;-data-export (last visited Nov. 11, 2020) (stating, "[t]hese terms reflect the parties' agreement with respect to the terms governing processing and security of Customer Data under the [Firebase Terms of Service for Firebase Services"] Agreement."). *See also* Terms of Service for Firebase Services, FIREBASE, https://firebase.google.com/terms (last visited Nov. 11, 2020) (stating, "I agree that my use of Firebase service is subject to the applicable terms below," including the "Firebase Data Processing and Security Terms").

Terms is to give app developers (and regulators, as further discussed below) the assurance that users can limit Google's data collection from Google's "Privacy Controls" as required by recent privacy laws.[44] Such Terms state that "[i]f Non-European Data Protection Legislation applies to either party's processing of Customer Personal Data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that Customer Personal Data."[45]

109. The California Consumer Privacy Act ("CCPA"), CIPA, the CDAFA, and the FTC Act (as implemented through the FTC Consent Decree) each qualifies as "Non-European Data Protection Legislation."[46] These laws forbid Google from using the Firebase SDK scripts to collect consumers' communications with apps without their consent. Therefore, Google's "Firebase Data Processing And Security Terms" indicated to developers (wrongly) that Google's "Web & App Activity" feature, when turned to "off," would prevent Google from collecting its users' communications with their apps.

110. Accordingly, app developers implementing Firebase SDK have not consented, do not consent, and cannot consent to Google's interception and collection of user data for Google's own purposes when users have turned off "Web & App Activity." In any event, consent to such brazen data-collection activities must be specific and express. There is no disclosure or service agreement between Google and third-party app developers that grants Google permission to intercept communications between users and apps when the user has turned off the "Web & App Activity" feature. And Google provided no notice to third-party app developers that it would intercept communications between users and apps when users shut off "Web & App Activity."

---

[44] See also Google Ads Data Processing Terms, GOOGLE BUSINESSES AND DATA, https://privacy.google.com/businesses/processorterms/, Section 9, providing similar promises of honoring data subject rights and providing controls via "Data Subject Tool(s)" to control data collection (last visited Nov. 11, 2020).

[45] Firebase Data Processing and Security Terms, FIREBASE, https://firebase.google.com/terms/data-processing-terms#9.-data-subject-rights;-data-export (last visited Nov. 11, 2020), Section 5.1.3.

[46] The term is defined, in Google's terms, as "data protection or privacy legislation in force outside the European Economic Area, Switzerland, and the UK." Firebase Data Processing and Security Terms, FIREBASE, https://firebase.google.com/terms/data-processing-terms#9.-data-subject-rights;-data-export (last visited Nov. 11, 2020).

111. Further, nowhere in any disclosures did Google ever indicate to its users that any separate agreement, between Google and an app developer, might override the user's decision to turn off Web & App Activity.

IV. Google Profits from the Communications It Intercepts Using Firebase SDK

112. Google's continuous tracking of users is no accident. Google is one of the largest technology companies in the world. Google LLC and its parent Alphabet Inc. have over 1.5 billion active account users, and Alphabet Inc. boasts a net worth exceeding $1 trillion.

113. Google's enormous financial success results from its unparalleled tracking and collection of personal and sensitive user information (including Plaintiffs' and Class members'), which data Google then uses to target its advertisements.

114. Over the last five years, virtually all of Google's revenue was attributable to third-party advertising. Google is continuously driven to find new and creative ways to leverage users' data in order to sustain Google's phenomenal growth in its sales of advertising services.

115. Google profits from the data it collects—including the data collected from apps while users have switched off the "Web & App Activity" feature—in at least three ways. First, Google associates the confidential communications and data with a user profile or profiles. Second, Google later uses the user's profile (including the intercepted confidential communications at issue here) to direct targeted advertisements to consumers (including Plaintiffs and Class members). Third, Google uses the results to modify Google's own algorithms and technology, such as Google Search.

A. Google Creates and Maintains "Profiles" on Its Users Using the Data Collected from Firebase SDK

116. Google builds and maintains "profiles" relating to each individual (including Plaintiffs and Class members) and to each of their devices. These "profiles" contain all the data Google can collect associated with each individual and each device. In a *Wired* article regarding Google's privacy practices, Professor Schmidt stated that Google's "business model is to collect as much data about you as possible and cross-correlate it so they can try to link your online persona with your offline persona. This tracking is just absolutely essential to their business. 'Surveillance

capitalism' is a perfect phrase for it."[47]

117. Google uses those user profiles for numerous purposes. One important purpose is to guide Google's targeted advertisements. The profiles allow Google to effectively target advertisements. As a result of using the user profiles, Google's targeted advertisements are more effective and therefore Google can charge advertisers more for these services.

118. Google includes in its user profiles data secretly transmitted to Google from consumer devices by the Firebase SDK scripts during times that the user had switched the "Web & App Activity" feature off. By including this data in its user profiles, Google increases the user profiles' value to Google and thereby allows Google to more effectively target advertisements to these users (among other uses of these profiles).

119. Google combines the data, transmitted to Google by the Firebase SDK scripts, with additional data generated by apps, running on the device, that use Google's services. This additional data includes: (1) device identifiers from the device's operating system; (2) geolocation information, including from cellular and wi-fi signals, and (3) Google's own persistent identifiers, such as its Google Analytics User-ID and Chrome X-Client Referrer Header, which identify specific individual users and the users' devices.

120. The following diagram illustrates the process by which Google collects information from a mobile device while users have Web & App Activity turned off:

//

//

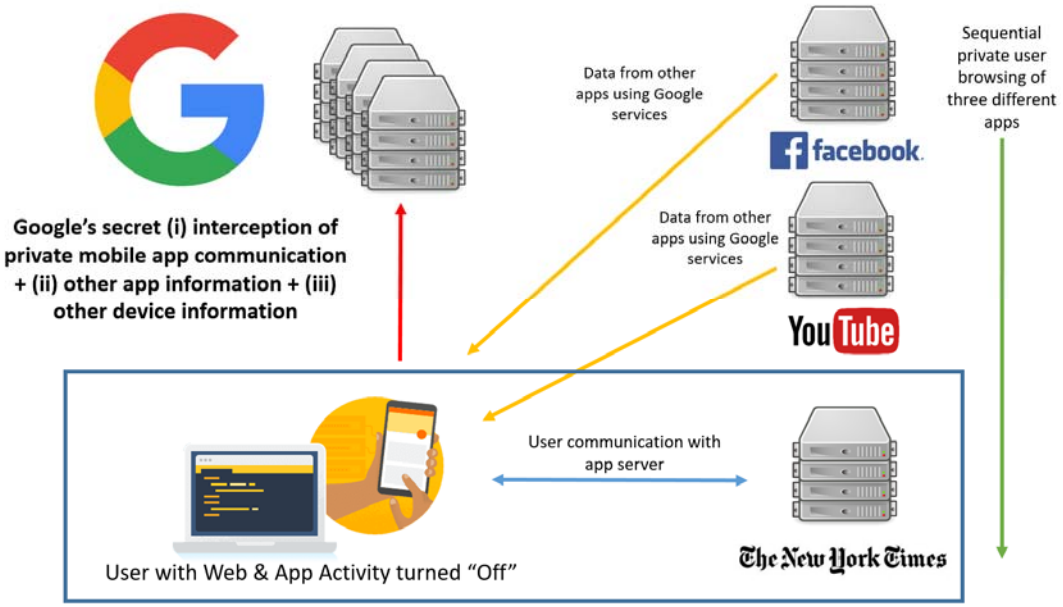
//

//

//

//

[47] Lily Hay Newman, *The Privacy Battle to Save Google from Itself*, WIRED (Nov. 1, 2018), https://www.wired.com/story/google-privacy-data/ (last visited Nov. 11, 2020).



121. The communications and data transmitted to Google from consumer devices, by the Firebase SDK scripts, is not "anonymized" in any meaningful sense of that word. Instead, this data is combined by Google into a user profile with all the other detailed, user-specific data Google collects on individuals and their devices. Google then uses these detailed profiles to help generate billions of dollars in advertising revenues without users' consent.

B. Google Generates Targeted Advertising to Class Members Based on Data Transmitted to Google by the Firebase SDK Scripts

122. Google's targeted advertising services generate the vast majority of Google's hundreds of billions of dollars in annual revenue.[48] The more accurately that Google can track and target consumers, the more advertisers are willing to pay.

123. Google's "Ad Manager" service generates targeted advertisements to be displayed alongside third-party websites' content. The "user profiles" described above are used by Ad Manager to select which ads to display to users.

124. Google also sells in-app advertising services. For example, some apps display an

[48] Eric Rosenberg, *How Google Makes Money (GOOG)*, INVESTOPEDIA (June 23, 2020), *available at* https://www.investopedia.com/articles/investing/020515/business-google.asp#:~:text=Google%20Ads%20and%20Search%20Advertising,results%20generated%20by%20Google's%20algorithm (last visited Nov. 11, 2020).

advertisement on part of the screen. Google is paid to select and transmit targeted advertisements in this way, as well. In doing so, Google uses the "user profiles" described above.

125. Google is able to demand high prices for its targeted-advertising services because Google's user profiles (including data that Google obtained from the Firebase SDK transmissions) are so detailed.

126. If Google were to give consumers (including Plaintiffs and Class members) power to shut off the stream of data transmission from Firebase SDK, then that would harm Google's ability to build detailed user profiles and to effectively target advertisements. That, in turn, would harm Google's biggest (by far) source of revenue. This explains why Google repeatedly promises privacy and control (in order to make users feel better) and then repeatedly breaks those promises (in order to make billions of dollars).

C. Google Refines and Develops Products Using the Data Transmitted to Google by the Firebase SDK Scripts

127. Google also benefits by using the data it collects to refine existing Google products, services, and algorithms—and to develop new products, services, and algorithms. This collection, usage, and monetization of user data contravenes the steps Plaintiffs and Class members have taken to try to control their information and to prevent it from being used by Google.

1. Google Search

128. Currently, more than 90% of online searches carried out by U.S. consumers are done using Google's web-based search engine, called Google Search.

129. Google Search, and the algorithms that power it, make use of the data Google has obtained from the Firebase SDK transmissions at issue here. Google Search would not be nearly as effective without the Firebase SDK data at issue here.

2. On-Device Search Features

130. Google also uses the Firebase SDK transmissions to develop and refine Google's "On-Device Search" services. "On-Device Search" refers to a search of the content contained, linked, or referred to in the various apps of a mobile device. On most devices, this function appears as a text rectangle, with a magnifying glass on the left side, and the word "Search" appearing where

the user is meant to type in the query.

131. A well-built On-Device Search feature will not only allow users to find their tools and apps, but will also "deep link" the user to specific content and pages within the device's apps. These "deep links" are similar to how web-based searches, like Google Search, can take a user directly to specific pages within a website. If a user then selects a search result that is "deep linked" to content on an app, the phone will respond to that selection by opening the relevant app and taking the user to the relevant content within the app. This is in contrast to the more traditional Google Search function, which would only search *web pages* rather than searching *within apps.*

132. In 2015, an industry publication named *Search Engine Watch* described Google's On-Device Search as follows: "Google can index the content contained within an app, either through a sitemap file or through Google's Webmaster Tools. If someone searches for content contained within an app, and if the user has that app installed, the person then has the option to view that content within the app, as opposed to outside the app on a mobile webpage. For sites that have the same content on their main website and app, the app results will appear as deep links within the search listing. If the user has the app installed and they tap on these deep links, the app will launch and take them directly to the content."[49]

133. In order to make its On-Device Search function more powerful, Google collects and records the content of apps on users' phones. This is called "indexing." By "indexing" the contents of apps, Google makes On-Device search quicker and more accurate. In August 2015, Google-sponsored publication *Search Engine Land* announced:

> Historically, *app landing pages* on websites have been in the Google index—but *actual apps* and *internal app screens* have not…. Now that Google is indexing both app landing pages and deep screens in apps, Google's app rankings fall into two basic categories, App Packs and App Deep Links. App Packs are much more like the app search results that SEOs [search engine optimizers] are used to, because they link to app download pages in Google Play or the App Store, depending on the device that you are

[49] Christopher Ratcliff, *What Is App Indexing and Why Is It Important?*, SEARCH ENGINE WATCH (Nov. 19, 2015), *available at* https://www.searchenginewatch.com/2015/11/19/what-is-app-indexing-and-why-is-it-important/ (last visited Nov. 11, 2020).

searching from."[50]

134. In March 2015, the industry publication *Readwrite* reported on a rival search function, called AppWords, that was outperforming Google in the market for On-Device Search:

> Deep links for mobile apps were designed to mimic Web links by letting users click into different parts of an app and not just its home screen. But they're also changing the way we discover new things. The deep-linking startup Deeplink has launched what appears to be the first intent based and keyword driven mobile search. Called AppWords (a play on Google AdWords), the new service basically prompts new links for app users to click on—ones that will take them from one app directly into another that's already on their phone. "Query-based search has become a secondary surfacing tool in mobile," said cofounder Noah Klausman. "AppWords uses context to predict what people want to search. What we've built is what Google should have built a long time ago."[51]

135. Google responded to this competition by acquiring Firebase in 2014, and then launching the Firebase SDK platform. Google intentionally designed the Firebase SDK scripts to copy and transmit, to Google, users' communications with the apps and app developers while overriding device and account level controls. Google did this because Google knew that it needed this data to develop and refine Google's On-Device Search services. The Firebase SDK scripts give Google massive amounts of user data from apps—including apps that were developed for the devices of Google's rival, Apple.

136. When app developers use Firebase SDK, Google receives a number of benefits that enhance and reinforce its market power in the market for On-Device Search. As Google states in its own technical documentation for Firebase, Google's On-Device Search "uses information about the actions users take on public and personal content in an app to improve ranking for Search results and suggestions."

//

---

[50] Emily Grossman, *App Indexing & The New Frontier of SEO: Google Search + Deep Linking*, Search Engine Land (Aug. 12, 2015), *available at* https://searchengineland.com/app-indexing-new-frontier-seo-google-search-deep-linking-226517 (last visited Nov. 11, 2020).

[51] Lauren Orsini, *How Deep Linking Can Change the Way We Search on Mobile*, READWRITE.COM (Mar. 24, 2015), *available at* https://readwrite.com/2015/03/24/deep-linking-search-appwords/ (last visited Nov. 11, 2020).

V. The Communications Intercepted by Google Using Firebase SDK Are Highly Valuable

137. The information Google has collected using Firebase SDK is highly valuable to Google, to other technology and advertising companies, and to users. This value is well understood in the e-commerce industry.[52] The world's most valuable resource is no longer oil, but is instead consumers' data.[53]

138. Even before the Class Period, there was a growing consensus that consumers' personal data was very valuable. In 2004, Professor Paul M. Schwartz noted in the *Harvard Law Review*:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.[54]

139. Likewise, in 2011, Christopher Soghoian (a former fellow at the Open Society Institute and current principal technologist at the ACLU) wrote in *The Wall Street Journal*:

---

[52] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS No. 220 at 7 (Apr. 2, 2013), *available at* http://dx.doi.org/10.1787/5k486qtxldmq-en; *Supporting Investment in Knowledge Capital, Growth and Innovation*, OECD at 319 (Oct. 13, 2013), *available at* https://www.oecd.org/sti/inno/newsourcesofgrowthknowledge-basedcapital.htm; Pauline Glickman & Nicolas Glady, *What's the Value of Your Data?* TECHCRUNCH (Oct. 13, 2015), *available at* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited Nov. 11, 2020) Paul Lewis & Paul Hilder, *Former Cambridge Analytica Exec Says She Wants Lies to Stop*, THE GUARDIAN (March 23, 2018), *available at* https://www.theguardian.com/uk-news/2018/mar/23/former-cambridge-analytica-executive-brittany-kaiser-wants-to-stop-lies (last visited Nov. 11, 2020); SHOSHANNA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER at 166 (2019).

[53] *The World's Most Valuable Resource Is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), *available at* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Nov. 11, 2020).

[54] Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056–57 (2004).

> The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online.
>
> Although we now regularly trade our most private information for access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.[55]

A. The Firebase SDK Transmissions Are Valuable to Class Members

140. It is possible to quantify the cash value, to Class members, of the communications and data collected by Google using the Firebase SDK scripts while the "Web & App Activity" feature was turned off by Class members.

141. For example, in a study authored by Tim Morey, researchers studied the value that 180 internet users placed on keeping personal data secure.[56] Contact information was valued by the study participants at approximately $4.20 per year. Demographic information was valued at approximately $3.00 per year. However, web browsing histories were valued at a much higher rate: $52.00 per year. The chart below summarizes the findings:

//

//

//

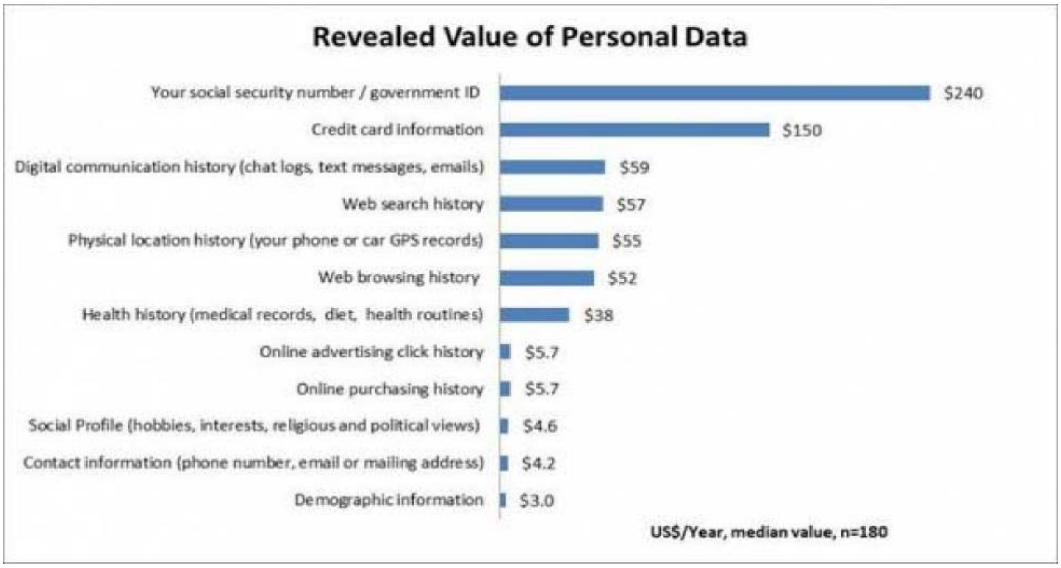
//

//

---

[55] Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE WALL STREET JOURNAL (Nov. 15, 2011), *available at* https://www.wsj.com/articles/SB10001424052970204190704577024262567105738 (last visited Nov. 11, 2020).

[56] Tim Morey, *What's Your Personal Data Worth?*, DESIGN MIND (Jan. 18, 2011), *available at* https://web.archive.org/web/20131206000037/http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html (last visited Nov. 11, 2020).



Although none of the categories on this chart corresponds directly to the data obtained by Google from Class members using the Firebase SDK scripts, Morey's research demonstrates that it is possible, in theory, to quantify the value of this data to users.

B. The Firebase SDK Transmissions Are Valuable to Google

142. In addition to quantifying the value of the intercepted data *to users*, it is also possible to quantify the value of this data *to Google*.

143. For example, it is possible to calculate the profits Google has earned from using this data to enhance its "user profiles"; to sell targeted advertisements; and to develop and refine other Google products. *See supra*, ¶¶ 112-36.

144. It is also possible to assess the value of the intercepted data to Google by reference to the money that Google has, on other occasions, paid to users for this kind of data. Google began paying users for their web browsing data in 2012.[57]

[57] Jack Marshall, *Google Pays Users for Browsing Data*, DIGIDAY (Feb. 10, 2012), *available at* https://digiday.com/media/google-pays-users-for-browsing-data/ (last visited Nov. 11, 2020); *see also* K.N.C., *Questioning the Searchers*, THE ECONOMIST (June 13, 2012), *available at* https://www.economist.com/schumpeter/2012/06/13/questioning-the-searchers (last visited Nov. 11, 2020).

145. Google also pays internet users to participate in a panel that Google calls "Google Screenwise Trends." The purpose of this panel is, according to Google, "to learn more about how everyday people use the Internet."

146. Upon becoming panelists for Google Screenwise Trends, these users add a browser extension that shares with Google the sites they visit and how they use them. The panelists consent to Google tracking such information for three months in exchange for one of a number of "gifts," including gift cards to retailers such as Barnes & Noble, Walmart, and Overstock.com. After three months, Google then pays panelists additional gift cards "for staying with" the panel.

147. These gift cards, mostly valued at $5, demonstrated that Google assigned cash value to the data it obtained from internet users' communications with the websites they visited. Google now pays Screenwise panelists up to $3 *per week*.

148. There are other ways to assess the value of this data, including in terms of Google's ability to maintain and extend its monopolies, as discussed below.

C. The Firebase SDK Transmissions Would Be Valuable to Other Internet Firms

149. The Firebase SDK transmissions at issue in this case would have value to other internet firms besides Google. It is possible to quantify this value.

150. During the Class Period, a number of platforms have appeared on which consumers monetize their data. For example:

a. Brave's web browser pays users to watch online targeted ads, while blocking out everything else.[58]

b. Loginhood "lets individuals earn rewards for their data and provides website owners with privacy tools for site visitors to control their data sharing," via a "consent

[58] Brandan Hesse, *Get Paid to Watch Ads in the Brave Web Browser*, LIFEHACKER (Apr. 26, 2019), *available at* https://lifehacker.com/get-paid-to-watch-ads-in-the-brave-web-browser-1834332279#:~:text=Brave%2C%20a%20chromium-based%20web%20browser%20that%20boasts%20an,a%20more%20thoughtful%20way%20than%20we%E2%80%99re%20accustomed%20to (last visited Nov. 11, 2020) ("The model is entirely opt-in, meaning that ads will be disabled by default. The ads you view will be converted into Brave's cryptocurrency, Basic Attention Tokens (BAT), paid out to your Brave wallet monthly").

manager" that blocks ads and tracking on browsers as a plugin.[59]

c. Ex-presidential candidate Andrew Yang's "Data Dividend Project" aims to help consumers, "[t]ake control of your personal data. If companies are profiting from it, you should get paid for it."[60]

d. Killi is a new data exchange platform that allows users to own and earn from their data.[61]

e. BIGtoken "is a platform to own and earn from your data. You can use the BIGtoken application to manage your digital data and identity and earn rewards when your data is purchased."[62]

f. The Nielsen Company, famous for tracking the behavior of television viewers' habits, has extended its reach to computers and mobile devices through Nielsen Computer and Mobile Panel. These applications track consumers' activities on computers, phones, tablets, e-readers, and other mobile devices. In exchange, Nielsen gives users points worth up to $50 per month, plus the chance of winning more money in regular sweepstakes.[63]

---

[59] *Privacy Drives Performance*, LOGINHOOD, https://loginhood.io/ (last visited Nov. 11, 2020); *see also Chrome Browser Extension*, LOGINHOOD, https://loginhood.io/product/chrome-extension (last visited Nov. 11, 2020) ("Start earning rewards for sharing data – and block others that have been spying on you. Win-win.").

[60] *Your Data - Your Property*, DATA DIVIDEND PROJECT, https://www.datadividendproject.com/ (last visited Nov. 11, 2020) ("Get Your Data Dividend . . . . We'll send you $$$ as we negotiate with companies to compensate you for using your personal data.").

[61] *Killi Paycheck*, KILLI, https://killi.io/earn/ (last visited Nov. 11, 2020).

[62] *FAQ*, BIG TOKEN, https://bigtoken.com/faq#general_0 (last visited Nov. 11, 2020) ("Third-party applications and sites access BIGtoken to learn more about their consumers and earn revenue from data sales made through their platforms. Our BIG promise: all data acquisition is secure and transparent, with consumers made fully aware of how their data is used and who has access to it.").

[63] Kevin Mercandante, *Ten Apps for Selling Your Data for Cash*, BEST WALLET HACKS (June 10, 2020), *available at* https://wallethacks.com/apps-for-selling-your-data/ (last visited Nov. 11, 2020).

g. Facebook has an app, called "Study," that pays users for their data. Facebook has another app, called "Pronunciations," that pays users for their voice recordings.[64]

151. As established by the California Constitution and the CCPA, and recognized by the recently-enacted California Privacy Rights and Enforcement Act, consumers have a property interest in their personal data. Not only does the CCPA prohibit covered businesses from discriminating against consumers that opt-out of data collection, the CCPA also expressly provides that: "[a] business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information." Cal. Civ. Code § 1798.125(b)(1). The CCPA provides that, "[a] business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature." Cal. Civ. Code § 1798.125(b)(4).

152. Through its false promises and unlawful data collection, Google is unjustly enriching itself.

153. If not for Google's actions, consumers could have received monetary value for their data from other internet firms.

D. There Is Value to Class Members in Keeping Their Data Private

154. In addition to monetary value of *selling* their data, Class members also assign value to keeping their data *private.* It is possible to quantify this privacy value, which is destroyed when the Firebase SDK scripts surreptitiously transmit users' data to Google while the users have turned off the "Web & App Activity" feature.

155. According to Google, more than 200 million people visit Google's "Privacy Checkup" website each year. Each day, nearly 20 million people check their Google privacy settings. Users do these things because they care about keeping their data private and preventing its disclosure to anyone else, including to Google.

---

[64] Jay Peters, *Facebook Will Now Pay You for Your Voice Recordings*, THE VERGE (Feb. 20, 2020), *available at* https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-prounnciations-app (last visited Nov. 11, 2020).

156. Users also switched off the "Web & App Activity" feature for the same reason—they cared about their privacy and wished to prevent anyone, including Google, from accessing their data.

157. Surveys of consumers indicate the importance that consumers assign to privacy. For example, in a recent study by the Pew Research Center, 93% of Americans said it was "important" for them to be "in control of who can get information" about them. Seventy-four percent said it was "very important." Eighty-seven percent of Americans said it was "important" for them not to have someone watch or listen to them without their permission. Sixty-seven percent said it was "very important." And 90% of Americans said it was "important" that they be able to "control[] what information is collected about [them]." Sixty-five percent said it was "very important" to control this.

158. Likewise, in a 2011 Harris Poll study, 76% of Americans agreed that "online companies, such as Google or Facebook, control too much of our personal information and know too much about our browsing habits."

VI. Google Acted Without Consent To Intercept and Collect User App Data to Maintain and Extend Its Monopolies

159. Google's audacious invasion of millions of users' privacy without consent was motivated in part by Google's ongoing efforts to unlawfully maintain and extend its monopoly power in search and other markets. These efforts included Google's 2014 acquisition of Firebase and Google's ongoing and unlawful interception, collection, and use of data when users have taken the affirmative step of turning off "Web & App Activity" to prevent such interception, collection and use.

A. Google's Web Dominance

160. Since its founding in 1998, Google has developed technology allowing Google to constantly track consumers across the internet, fueling and then ensuring Google's search dominance. Over 90% of the U.S. population uses Google to conduct web searches, giving Google an enormous and unprecedented set of consumer data.

161. Google's dominance is tied to and based in part on Google's massive advertising business. Over 70% of online websites and publishers on the internet utilize Google's website visitor-tracking product, "Google Analytics," which allows Google to track consumers.

162. To implement Google Analytics, Google requires websites to embed Google's custom code into their existing webpage code. Google's embedded code causes the user's browser to send his or her personal information to Google and its servers in California, such as the user's IP address, the URL address (which identifies the particular page of the website that is being visited), and other information regarding the user's device and browser.

163. By embedding its tracking code through Google Analytics, Google has been able to intercept, track, collect, take, compile, and use a staggering amount of consumer data, far more than any company in the world. Because more than 70% of websites use Google Analytics, Google is able to track and collect personal consumer data online in real time and on non-Google properties—more pervasively than any other company online.

164. Google has been able to maintain and extend its dominance in products like Google Search because no other company is able to track consumers and aggregate their communications with websites and throughout the internet like Google.

B. Google's Mobile Problem

165. Prior to 2007, with Apple's introduction of the iPhone, internet searching was primarily done on a computer, through a browser. With the 2007 launch of the iPhone, online activities began to move from computers to smartphones and the apps that run on them. This created an existential threat to Google's dominance.

166. Before Google acquired Firebase in October 2014, Google recognized that mobile applications on mobile devices allowed users to access information without using Google search. Google thus knew that it needed data from users' app browsing activities to protect its search dominance and advertising revenues.

167. In February 2014, Google stated in its 10-K filings that one competitive threat to Google was "[m]obile applications on iPhone and Android devices, which allows users to access information directly from a publisher *without using our search engines*."

168. Google identified one of the key risk factors for the company as more people "using devices other than desktop computers to access the internet" and acknowledged that "search queries are increasingly being undertaken via 'apps' tailored to particular devices or social media platforms, *which could affect our share of the search market over time*."

169. Google stated in its next series of 10-K filings that this risk was a threat to Google's lucrative advertising business, noting that "search queries are increasingly being undertaken via 'apps' tailored to particular devices or social media platforms, *which could affect our search and advertising business over time*."

C. Google's Mobile Focus with Android & Firebase

170. Google feared that consumers' switch from using computers to search, to instead using mobile devices to search, would endanger Google's dominance of the market for search functions. In response to that danger, Google adopted a new strategy: transport and embed Google's search ecosystem into every part of mobile devices over which Google had, or could gain, influence. Google's purpose in doing this was to keep fueling Google's dominance and advertising revenues.

171. One way Google sought to maintain and extend its dominance was with its acquisition of the Android operating system (OS); its subsequent development of Android; and its push to cause mobile device manufacturers to adopt Android on their devices. Google acquired Android in 2005 and released the first commercial version of the Android operating system, Android 1.0, in September 2008.

172. As recently recounted in the comprehensive report issued by the U.S. House of Representative's Subcommittee on Antitrust, Commercial and Administrative Law, entitled *Investigation of Competition In Digital Markets*, "[f]or mobile devices, Google imposed a set of restrictive contractual terms effectively requiring manufacturers of devices that used its Android operating system to pre-install both Chrome and Google Search."[65]

---

[65] STAFF OF S. COMM. ON ANTITRUST, COMMERCIAL, AND ADMINISTRATIVE LAW, INVESTIGATION OF COMPETITION IN DIGITAL MARKETS, at 178, https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519.

173. Just as Microsoft used its monopoly power on manufacturers to require the installation of Windows Explorer instead of Netscape, Google used its monopoly power to require phone manufacturers and app developers to incorporate Google's various products that reinforce Google Search. The more dominance Google could obtain in search, the more information it could collect and aggregate. The more information it could collect and aggregate, the more dominance Google could have in advertising, its key profit center.

174. One other way that Google sought to maintain and extend its dominance was with its October 2014 acquisition of Firebase; its subsequent development of the Firebase SDK platform; and its push to cause third-party app developers to adopt Firebase SDK. Before Google acquired it, Firebase was a separate company with an application programing interface (API) enabling synchronization of application data across Apple's iOS, Android, and web devices. By acquiring Firebase, Google gained the tools it needed to acquire users' mobile app data and, in part and along with Android, to address the competitive threat posed by Apple.

175. Firebase was so important to Google that the company featured it during Google's annual conference in May 2016, with Google CEO Sundar Pichai stating: "Firebase is the most comprehensive developer offering we have done to date." Google presented more than thirty sessions on Firebase during that 2016 conference.

176. During that conference, on May 20, 2016, Jason Titus, Vice President of Google's Developer Products Group, announced the "next generation of Firebase" with a mobile analytics tool called "Firebase Analytics" that was "inspired by much of the work that we've done in the last 10 years with Google Analytics, but it's designed specifically for the unique needs of apps."[66]

177. Google's Android and Firebase efforts are also tied to Google's efforts with "on device search." Because mobile apps are not constantly active on the device and need to be launched separately, it is much more difficult for Google to crawl and index content maintained on mobile content. Because of personal content and information, apps also tend to be secured,

---

[66] Pangambam S., *Google I/O 2016 Keynote (Full Transcript)*, THE SINGJU POST (May 20, 2016), *available at* https://singjupost.com/google-io-2016-keynote-full-transcript/?singlepage=1 (last visited Nov. 11, 2020).

self-contained, and separated from other apps. Unlike with data collection on the web, Google cannot simply send its army of "web crawlers" to scan, scrape, and store content with mobile apps.

178. Google's Firebase acquisition provided Google with what it previously lacked: the ability to collect personal user data *en masse* from mobile devices and apps—including devices and apps developed by its rival Apple. When app developers use Firebase SDK, Google receives a number of benefits that enhance and reinforce Google's market power. Firebase SDK enables Google to crawl and index apps just as it does for traditional websites. Developers often have no choice but to use Firebase SDK because of Google's demands and market power, including with search, analytics, advertisements, and the Android mobile operating system.

D. Google's Increasing Trove of Consumers' Mobile Data and Power

179. Since acquiring Firebase in 2014, Google has quietly collected what must be the largest index of mobile app pages in the world, including most apps on Android OS. Google has also continued to use its monopoly power with respect to web-based searching to push rapid adoption of Firebase SDK, so that it can eventually release a more complete search product that includes every mobile app page in the world. As a result, nearly every Android OS user (and most iOS users) are likely to have fallen victim to Google's unlawful acts.

180. Perhaps most concerning is that Google uses the data collected with Firebase SDK—including while users have Web & App Activity turned off—to target users with advertisements throughout Google's entire advertising ecosystem—including in the very app where the communication was intercepted, and other apps of other app developers. All consumers' requests for content from the app thereby become accessible, collectible, and usable by Google, even where users have not consented to Google's collection and use of such information.

181. By compiling not just consumer profiles, but surveying human behavior across the vast majority of mobile app activity, Google tracks consumer activity more pervasively than any other company and is thus able to create a more targeted search product as compared to its competitors, by its ability to claim that Google knows how best to rank websites and online properties. Google Search would not be nearly as potent a tool without Google Analytics as a complement and Google's ongoing data collection with its Firebase SDK.

182. Google's own internal documents reveal that Google knows what it is doing is wrong. But Google has made a bet: It has wagered that by the time regulators, lawmakers, or the public at large uncover that Google has compiled an almost unlimited amount of user data from apps (without proper consent), Google will have already won the game against any prospective competitor. Left unchecked, Google will achieve near complete monopoly power in search, data collection, and private user information the likes of which the world has never seen.

VII. Tolling of the Statutes of Limitations

183. Each unauthorized transmission of data to Google by the Firebase SDK scripts is a separate "wrong" which triggers anew the relevant statutes of limitations.

184. Moreover, any applicable statutes of limitations have been tolled under (1) the fraudulent concealment doctrine, based on Google's knowing and active concealment and denial of the facts alleged herein, and (2) the delayed discovery doctrine, as Plaintiffs did not and could not reasonably have discovered Google's conduct alleged herein until shortly before the original complaint was filed.

185. Throughout the Class Period, Google repeatedly and falsely represented that its users (including Plaintiffs and Class members) could prevent Google from intercepting their communications by turning off "Web & App Activity." Google never disclosed that it would continue to track users and collect their data once this feature was turned off.

186. Google also further misled users by indicating that data associated with them would be viewable through their account, but Google did not make the user data at issue in this lawsuit (collected while Web & App Activity is turned off) viewable in user accounts. Google's failure to do so during the Class period is part of Google's active deception and concealment.

187. Google has also made the statements quoted above, which (1) misrepresent material facts about Google's interception and use of users' data on apps and/or (2) omit to state material facts necessary to make the statements not misleading. *See supra*, ¶¶ 86–104. Google thereby took affirmative steps to mislead Plaintiffs and others about the effect of switching the "Web & App Activity" feature off.

188. Plaintiffs relied upon Google's false and misleading representations and omissions and believed that Google was not intercepting their private communications while the "Web & App Activity" feature was turned off.

189. Plaintiffs did not discover and could not reasonably have discovered that Google was instead intercepting and using their data in the ways set forth in this Complaint until shortly before the lawsuit was filed in consultation with counsel.

190. Plaintiffs exercised reasonable diligence to protect their data from interception. That is precisely why they turned off the "Web & App Activity" feature: to protect their data from interception by Google. Plaintiffs did not and could not reasonably have discovered their claims until consulting with counsel shortly before the filing of the original complaint through the exercise of reasonable diligence.

191. Accordingly, Plaintiffs and Class members could not have reasonably discovered the truth about Google's practices until shortly before this litigation was commenced.

VIII. Google Collected the Data for the Purpose of Committing Further Tortious and Unlawful Acts

192. Google collected the data at issue here (from users who turned off "Web & App Activity") for the purpose of committing additional tortious and unlawful acts. Google's subsequent use of the data violated the California Consumer Privacy Act ("CCPA"); the CDAFA; and the FTC's 2011 Consent Order. Google also used the data to tortiously invade consumers' privacy and intrude on their seclusion.

193. ***Google collected the data with the intent to violate the California Consumer Privacy Act.*** The data collected from users at issue in this lawsuit, while Web & App Activity is turned off, qualifies as "personal information" that is protected by the CCPA. Cal. Civ. Code § 1798.140(o). The CCPA provides:

> "A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not . . . use personal information collected for additional purposes without providing the consumer with notice consistent with this section."

Cal. Civ. Code § 1798.100(b) (emphasis added).

194. At the time Google collected data from users when they turned off "Web & App Activity," Google intended to "use" that data "for additional purposes without providing the consumer with notice consistent with this section." Whenever Google uses the confidential communications wrongfully collected or aggregates it with other information to gain additional insight and intelligence, Google has violated the express prohibitions of the CCPA.

195. Moreover, Google carried out its intent: As described elsewhere in this Complaint, Google made use of the data it collected from users who turned off "Web & App Activity" for "additional purposes." The users had never been "informed" of those "additional purposes." Google never gave its users "notice consistent with" the CCPA's requirements regarding these "additional purposes" for which Google used the data collected from users who have turned off Web & App Activity.

196. ***Google collected the data with the intent to violate the FTC's 2011 Consent Order.*** The FTC ordered Google to obtain "express affirmative consent" from each user, "prior to any new or additional sharing" of a user's information that is "a change from stated sharing practices in effect at the time [Google] collected such information."

197. Google began the data collection and sharing at issue in this lawsuit after the 2011 Consent Order. At the time Google collected data from users who turned off "Web & App Activity," Google intended to share that data with third parties, in a manner that was very different from the "stated sharing practices" Google had disclosed to users. Google intended to do this without obtaining consent.

198. Moreover, Google carried out its intent: Google shared and/or sold the data, collected from users who turned off "Web & App Activity," with third-parties including Google's advertising customers. That sharing and/or selling of data contradicted Google's repeated assurances to users, described herein. Google shared this data without obtaining consent.

199. ***Google collected the data with the intent to violate the CDAFA.*** The CDAFA provides that it is a public offense to "without permission . . . make[] use of any data from a computer . . . ." Cal. Penal Code § 502.

200. At the time that Google caused the Firebase SDK scripts to transmit users' data to Google's servers, Google intended to later "make use of" that data to enhance Google's profiles on the users; to sell advertising services; to select and send targeted advertising; and for other purposes. Google then did "make use of" the data in these ways. These subsequent acts by Google were separate and independent violations of the CDAFA.

201. ***Google collected the data with the intent to intrude upon users' seclusion and invade their constitutional privacy.*** The California Constitution and common law protect consumers from invasions of their privacy and intrusion upon seclusion – in addition to newer privacy laws such as the CCPA.

202. Users of apps turned off "Web & App Activity" for the purpose of preventing others, including Google, from finding out what the users were viewing and reading on mobile apps. For example, users' app activities, while "Web & App Activity" have been turned off, may reveal: a user's dating activity; a user's sexual interests and/or orientation; a user's political or religious views; a user's travel plans; a user's private plans for the future (e.g., purchasing of an engagement ring). These are just a few of the many intentions, desires, plans, and activities that users intend to keep private when they turn off "Web & App Activity."

203. Users had a reasonable expectation that Google would do as it promised, and that Google would stop collecting data from the Firebase SDK scripts once users switched off the "Web & App Activity" switch.

204. By causing targeted advertisements to be sent to users and to users' devices, based on data Google collected while users turned off "Web & App Activity," Google has caused that data to be revealed to others and has thereby invaded the privacy and intruded upon the seclusion of the users whose data was collected while they expected to have privacy.

205. Google had the intent to send these targeted advertisements at the time that Google was collecting data from users who turned off "Web & App Activity."

FACTUAL ALLEGATIONS REGARDING THE NAMED PLAINTIFFS

206. Google does not disclose all of the apps that use Firebase SDK, and for which Google therefore collected or continues to collect users' data while they have Web & App Activity turned off, or the time period during which Google collected or continues to collect such data for any given app. Plaintiffs are therefore at this time unable to identify all apps that are relevant for purposes of this litigation. Google's Firebase website identifies the following apps as supported by Firebase SDK: The New York Times, NPR One, Halfbrick, Duolingo, Alibaba, Lyft, Venmo, The Economist, Trivago, Ctrip, Wattpad, and Gameloft.[67] Other sources indicate that over 1.5 million apps use Google's Firebase SDK. Discovery will reveal which of Plaintiffs' apps were or are supported by Firebase SDK, and for which Google intercepted and collection data without disclosure of consent while Web & App Activity was turned off.

207. Plaintiff JulieAnna Muniz is an adult domiciled in California and has an active Google account and had an active account during the Class Period.

208. At various times during the Class Period, Ms. Muniz accessed numerous app pages on the Internet containing content she was interested in on her Apple device while "Web & App Activity" was turned off. Those app pages were accessed through apps including, among others, Amazon Shopping, Apple Music, Facebook, Google Maps, Instagram, Lyft, NPR One, Pandora, Apple Podcasts, Scrabble, Shazam, Solitaire, Uber, Venmo, The Weather Channel, and YouTube. She sent and received communications through these apps on mobile devices which were computing devices that were not shared devices. Her communications with the apps that used Firebase SDK were intercepted and tracked by Google without her knowledge or consent.

209. Plaintiff Anibal Rodriguez is an adult domiciled in Florida and has active Google accounts and had active accounts during the Class Period.

210. At various times during the Class Period, Mr. Rodriguez accessed numerous app pages on the Internet containing content he was interested in on his Android device while "Web

[67] *See Firebase Helps Mobile and Web App Teams Succeed*, FIREBASE, https://firebase.google.com/.

& App Activity" was turned off. Those app pages were accessed through apps including, among others, Alarm Clock for Me, Alibaba, AliExpress, Amazon Shopping, Android TV, Applebee's, Aptoide, Assistant, Barcode Scanner, Baseball Superstars 2020, Best Buy, Burger King, Call of Duty, Chili's, ClassDojo, Clawee, Craigslist, Current, Dairy Queen, Domino's, DoorDash, Dosh, Drive, DroidCam, Duolingo, eBay, ES File Explorer, Fair, Fire TV, Fulldive VR, GIPHY, Glassdoor, GoMLS miami, GoodRx, Google Pay, Google Play Games, Groupon, Grubhub, Hangouts, Home, Ibotta, Indeed Job Search, Instagram, Instant Save, Jimmy John's, Kindle, Layout, Letgo, LinkedIn, Little Caesars, Lyft, McDonald's, MX Player, myCigna, Netflix, Ninja's Creed, OfferUp, Pandora, ParkMobile, PayPal, Pi Music Player, Pollo Tropical, Postmates, Prime Video, Publix, Publix Instacart, RaceTrac, RAR, Realtor.com, Repost, Retro Bowl, Samsung Members, Samsung Members v1, Samsung Notes, Samsung Pay, Samsung voice input, Sezzle, Shazam, Shop, Shopping, Skillshare, Slack, Sleep Cycle, Slingshot Stunt Driver, Smart Switch, Sonos S1, SOPlayer, SoundCloud, Square Point of Sale, Stack Colors, Stash, Steam, Stickman Parkour Platform, Stream, Target, The Grand Mafia, Tiles Hop, Time Zone Updater, Trip.com, Trivago, Truebill, Uber, Uber Eats, Udemy, USPS Mobile, VeSyncFit, Voice, Voice Recorder, Walmart, WhatsApp, Wish, Word, WordPress, Xfinity, Xfinity Mobile, Xfinity My Account, Yelp, Your Phone Companion, YouTube Music, YouTube VR, Zelle, Zillow, ZipRecruiter, Zoho Mail, and Zoom. He sent and received communications through these apps on mobile devices which were computing devices that were not shared devices. His communications with the apps that used Firebase SDK were intercepted and tracked by Google without his knowledge or consent.

211. Plaintiff Eliza Cambay is an adult domiciled in California and has active Google accounts and had active Google accounts during the Class Period.

212. At various times during the Class Period, Ms. Cambay accessed numerous app pages on the Internet containing content she was interested in on her Android device while "Web & App Activity" was turned off. Those app pages were accessed through apps including, among others, A to Z ECG Interpretation, ABC, All Trails, Amazon Shopping, Amazon Music, Angie's List, Atmosphere, Atmosphere Binaural Therapy, Audible, Baskin Robbins, BBC America, Better Help, BluHop, Bodies by Rachel, Bruster's, Calm, Canva, Chewy, Chick-fil-A, Chill, Clinicals,

Coffee Bean, Cooking Fever, Coursera, Craigslist, Dad Jokes, Daily Mail Online, Disney Plus, Dogo, Dropbox, eBay, Ecosia, Einstein Bros Bagels, EMAY Portable ECG Monitor, Epocrates, ESPN, Essential Oils & More, Etsy, Evite, Facebook, Faire, FastSave, Facebook Messenger, Fi, Frontpoint, Gametime, Gmail, Good on You, GoodRx Pro, Goodtime, Google Calendar, Google Chrome, Google Classroom, Google Drive, Google Duo, Google Keep, Google Meet, Google Photos, Google Sheets, Google Translate, Google Voice, GoToWebinar, Grubhub, Harrison's Manual, HBOMax, Headspace, Hulu, IdentityForce, Imprivata ID, Instagram, Instagram Repost Video & Photo, Kinecta FCU, Lasting, Later, Lyft, Messenger Kids, NCCN Guidelines, Netflix, Nextdoor, Nintendo Switch Parental Controls, NMB, NPR One, OfferUp, Oilsprimer, OpenTable, Outlook, PayPal, PDK Touch, Peet's, PetDesk, PetPage, Ping, Pinterest, Pomodoro, Preview, Prime Video, ProtonMail, Puppr, Redbox, Reddit, Revolve, Ring, Robinhood, Rover, Screen Filter, SeatGeek, ShareWaste, Shark Tracker - OCEARCH, Shopify, Shopify POS, Shutterfly Share Site, Signal, Sketch Photo, Sleep Sounds, Smule, Snellen Chart, SoundCloud, Spotify, Sprouts, Square, Square Pic, Starbucks, StubHub, Surfline, Target, Tender Greens, The Economist, The New York Times, The RealReal, Think Dirty, Ticketmaster, TikTok, Tiny Scanner, Travelzoo, Tuner-Pitched, UpToDate, USPSTF, Venmo, Verizon Voicemail, Viber, Vivino, Waze, WhatsApp, WikiEM, Wikipedia, Wordscapes, Yelp, Yoga Down Dog, YouTube, Zappos, Zelle, Zen Planner, and Zoom. She sent and received communications through these apps on mobile devices which were computing devices that were not shared devices. Her communications with the apps that used Firebase SDK were intercepted and tracked by Google without her knowledge or consent.

213. Plaintiff Sal Cataldo is an adult domiciled in New York and has active Google accounts had active Google accounts during the Class Period.

214. At various times during the Class Period, Mr. Catalo accessed numerous app pages on the Internet containing content he was interested in on his Android devices while "Web & App Activity" was turned off. Those app pages were accessed through apps including, among others, Accuweather, Acrobat Reader, Amazon Shopping, Among Us, Aqua Mail, Audible, CBS Sports Fantasy, Chrome, Clock, Discord, Docs, Drive, ESPN, FuboTV, Gmail, IMDB, Instagram,

Jaybird, Kindle, Lawnchair, Maps, MyFitnessPal, Nest, Noom, NPR News, NPR One, The New York Times, Outlook, PayPal, Photos, Play Music, Play Store, Pocket, Pocket Casts, Pokerrr 2, Premier League, Relay for Reddit, Samsung Internet, Samsung Notes, Sheets, Slack, Smokeball, Spotify, Talon, Tesla, Textra, The Athletic, The Economist, TheScore, Uber, Venmo, WalletHub, Waze, WhatsApp, Whole Foods, WHOOP, Wikipedia, Yahoo Fantasy, YouTube, Zero Calorie Counter, and Zoom. He sent and received communications through these apps on mobile devices which were computing devices that were not shared devices. His communications with the apps that used Firebase SDK were intercepted and tracked by Google without his knowledge or consent.

215. Plaintiff Emir Goenaga is an adult domiciled in Florida and has an active Google account and had an active Google account during the Class Period.

216. At various times during the Class Period, Mr. Goenaga accessed numerous app pages on the Internet containing content he was interested in on his Apple device while "Web & App Activity" was turned off. Those app pages were accessed through apps including, among others, Acrobat, Amazon Shopping, American Airlines, Apple TV, Google Assistant, Microsoft Authenticator, Bible, Burger King, Cardiogram, Domino's, Dropbox, eBay, Ecobee, Facebook, Facebook Messenger, Fitness, Fly Delta, Google, Google Maps, Google Photos, HBO Max, Home Depot, IHG, Instagram, Key Ring, LinkedIn, Lyft, Macy's, Menchie's, Military Star Mobile, myAT&T, MySchoolBucks, Netflix, NPR One, Pandora, ParkMobile, PayByPhone, PayPal, Pizza Hut, QR Reader, Roblox, Scam Shield, Scanner App: PDF Document Scan, Shazam, Snapchat, Strava, SunPass, Sweatcoin, The New York Times, T-Mobile, T-Mobile Tuesdays, Turbo, Uber, USAA, Venmo, VideoConnect, Walgreens, Watch (Apple), Microsoft Word, Yahoo Mail, YouTube, and Zoom. He sent and received communications through these apps on mobile devices which were computing devices that were not shared devices. His communications with the apps that used Firebase SDK were intercepted and tracked by Google without his knowledge or consent.

217. Plaintiff Julian Santiago is an adult domiciled in Florida and has an active Google account and had an active Google account during the Class Period.

218. At various times during the Class Period, Mr. Santiago accessed numerous app pages on the Internet containing content he was interested in on his Apple device while "Web &

App Activity" was turned off. Those app pages were accessed through apps including, among others, Acorns, Amazon Shopping, Amazon Prime Video, Bleacher Report, Calm, Duolingo, E*Trade, ESPN Fantasy, Fundrise, Google Docs, Google Maps, Google Sheets, LinkedIn, MapMyRide, Marcus, Nextdoor, NFL, Nike Run Club, NPR One, Oak, Spotify, Starbucks, Stocks, Target, The Economist, Titan, Twitter, Venmo, Weather - The Weather Channel, Xfinity Stream, and YouTube. He sent and received communications through these apps on mobile devices which were computing devices that were not shared devices. His communications with the apps that used Firebase SDK were intercepted and tracked by Google without his knowledge or consent.

219. Plaintiff Harold Nyanjom is an adult domiciled in Kansas and has active Google accounts and had active Google accounts during the Class Period.

220. At various times during the Class Period, Mr. Nyanjom accessed numerous app pages on the Internet containing content he was interested in on his Android device while "Web & App Activity" was turned off. Those app pages were accessed through apps including, among others, Alibaba, Amazon Shopping, Android Accessibility Suite, Android Auto, Android System WebView, Audio Recorder, Auntie Anne's, B. Good, Booking.com, Boxer, Cash App, CBS, Chrome, Cricket Partner Tab, Digital Wellbeing, Dillon's, Docs, Dollar General, Duo, Duolingo, Emergency Alerts, Facebook, Facebook App Installer, Facebook App Manager, Facebook Services, Files, Files by Google, Firehouse Subs, Gallery, Game Launcher, Gmail, Google, Google Drive, Google Play Movies & TV, Google Play Services, Google Play Services for AR, Google Play Store, Google Text-to-Speech Engine, Home, Instacart, Instagram, Lens, Lyft, Maps, Messaging, Messenger, Mobile Service, Music, myCricket, News Break, NPR One, Outlook, Photos, QR Scanner, QuickMemo+, Repost, Sheets, SIM Toolkit, Slides, SmartWorld, Sricam, The Economist, The New York Times, TheSCOOP, TikTok, Trip.com, Trivago, Twitter, Uber, Visual Voicemail, Wattpad, WhatsApp, WordPress, Your Phone Companion, YouTube, and YouTube Music. He sent and received communications through these apps on mobile devices which were computing devices that were not shared devices. His communications with the apps that used Firebase SDK were intercepted and tracked by Google without his knowledge or consent.

221. Plaintiff Kellie Nyanjom is an adult domiciled in Kansas and has active Google accounts and had active Google accounts during the Class Period.

222. At various times during the Class Period, Ms. Nyanjom accessed numerous app pages on the Internet containing content she was interested in on her Android devices while "Web & App Activity" was turned off. Those app pages were accessed through apps including, among others, Alibaba, Amazon Shopping, Android Accessibility Suite, Android Auto, Android System WebView, Assistant, Audio Recorder, Auntie Anne's, B. Good, Booking.com, Boxer, Calculator, Calendar, Camera, Candy Crush Saga, Cash App, CBS, Chrome, Cricket Partner Tab, Digital Wellbeing, Dillon's, Docs, Dollar General, Duolingo, Emergency Alerts, Facebook, Facebook App Installer, Facebook App Manager, Facebook Lite, Facebook Services, Files, Files by Google, Firehouse Subs, Gallery, Game Launcher, Games, Gmail, Google, Google Drive, Google Go, Google Play Movies & TV, Google Play Services, Google Play Services for AR, Google Play Store, Google Text-to-Speech Engine, Home, Instacart, Instagram, Lens, LGE PAI Configuration, Lyft, Maps, Maps Go, Messaging, Messenger, Mobile Service, myCricket, News Break, NPR One, Outlook, Pandora, Pinterest, Play Music, Play Store (Google), QR Scanner, QuickMemo+, Repost, Sheets, SIM Toolkit, Slides, SmartNews, SmartWorld, Sricam, The Economist, The New York Times, TheSCOOP, TikTok, Trip.com, Trivago, Twitter, Uber, Visual Voicemail, Wattpad, WhatsApp, WordPress, Your Phone Companion, YouTube, and YouTube Music. She sent and received communications through these apps on mobile devices which were computing devices that were not shared devices. Her communications with the apps that used Firebase SDK were intercepted and tracked by Google without her knowledge or consent.

223. Plaintiff Susan Lynn Harvey is an adult domiciled in California and has active Google accounts and had active Google accounts during the Class Period.

224. At various times during the Class Period, Ms. Harvey accessed numerous app pages on the Internet containing content she was interested in on her Android devices while "Web & App Activity" was turned off. Those app pages were accessed through apps including, among others, Avast Cleanup, Avast Antivirus – Scan & Remove Virus, Cleaner, Bixby Vision, California Lottery, Candy Crush, EECU, Facebook Messenger, File Viewer for Android, Galaxy Themes,

Gangstar 4, Gold Fish, Google One, Jackpot Party, Jetpack, MixerBox, PicCollage, Samsung Gallery, Samsung Print Service Plugin, The New York Times, Voice Recorder, and Wattpad. She sent and received communications through these apps on mobile devices which were computing devices that were not shared devices. Her communications with the apps that used Firebase SDK were intercepted and tracked by Google without her knowledge or consent.

225. None of the Plaintiffs consented to the interception of their confidential communications made while "Web & App Activity" was turned off.

CLASS ACTION ALLEGATIONS

226. This is a class action pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure on behalf of the following Classes:

- Class 1 – All individuals who during the Class Period (a) turned off "Web & App Activity," and (b) whose mobile app activity was still transmitted to Google, from (c) a mobile device running the Android operating system (OS), because of Firebase SDK scripts, on a non-Google branded mobile app.

- Class 2 – All individuals who during the Class Period (a) turned off "Web & App Activity," and (b) whose mobile app activity was still transmitted to Google, from (c) a mobile device running a *non*-Android operating system (OS), because of Firebase SDK scripts, on a non-Google branded mobile app.

The Class Period begins on the date Google first received data, as a result of a Firebase SDK script, from the device of a user who had turned off (or paused) the "Web & App Activity" feature. The Class Period continues through the present.

227. Excluded from the Classes are: (1) the Court (including any Judge or Magistrate presiding over this action and any members of their families); (2) Defendant, its subsidiaries, parents, predecessors, successors and assigns, including any entity in which any of them have a controlling interest and its officers, directors, employees, affiliates, legal representatives; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel, Class counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

228. **Ascertainability**: Membership of the Classes is defined based on objective criteria and individual members will be identifiable from Google's records, including from Google's massive data storage, consumer accounts, and enterprise services. Based on information readily accessible to it, Google can identify members of the Classes who own an Android device or have a non-Android device with an associated Google account, who were victims of Google's impermissible interception, receipt, or tracking of communications as alleged herein.

229. **Numerosity**: Each of the Classes likely consists of millions of individuals. Accordingly, members of the Classes are so numerous that joinder of all members is impracticable. Class members may be identified from Defendant's records, including from Google's consumer accounts and enterprise services.

230. **Predominant Common Questions**: Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. Common questions for the Classes include, but are not limited to, the following:

a. Whether Google represented that Class members could control what communications of user information, app history and activity data were intercepted, received, or collected by Google;

b. Whether Google gave the Class members a reasonable expectation of privacy that their communications of user information, app history and activity data were not being intercepted, received, or collected by Google when the Class member had "Web & App Activity" turned off;

c. Whether Google in fact intercepted, received, or collected communications of user information, app history and activity data from Class members when the Class members had "Web & App Activity" turned off;

d. Whether Google's practice of intercepting, receiving, or collecting communications of user information, app history and activity data violated state and federal privacy laws;

e. Whether Google's practice of intercepting, receiving, or collecting

communications of user information, app history and activity data violated state and federal anti-wiretapping laws;

f. Whether Google's practice of intercepting, receiving, or collecting communications of user information, app history and activity data violated any other state and federal tort laws;

g. Whether Plaintiffs and Class members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

h. Whether Plaintiffs and Class members have sustained damages as a result of Google's conduct and if so, what is the appropriate measure of damages or restitution.

231. **Typicality**: Plaintiffs' claims are typical of the claims of other Class members, as all members of the Classes were uniformly affected by Google's wrongful conduct in violation of federal and state law as complained of herein.

232. **Adequacy of Representation**: Plaintiffs will fairly and adequately protect the interests of the members of the Classes and have retained counsel that is competent and experienced in class action litigation, including nationwide class actions and privacy violations. Plaintiffs and their counsel have no interest that is in conflict with, or otherwise antagonistic to the interests of the other Class members. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and they have the resources to do so.

233. **Superiority**: A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. This proposed class action presents fewer management difficulties than individual litigation and provides the benefits of a single adjudication, economies of scale and comprehensive supervision by a single, able court. Furthermore, as the damages individual Class members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for Class members to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

234. **California Law Applies to the Entirety of Both Classes**: California's substantive laws apply to every member of the Classes, regardless of where in the United States the Class member resides, or to which Class the Class member belongs. Defendant's own Terms of Service explicitly state, "California law will govern all disputes arising out of or relating to these terms, service specific additional terms, or any related services, regardless of conflict of laws rules. These disputes will be resolved exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts." By choosing California law for the resolution of disputes covered by its Terms of Service, Google concedes that it is appropriate for this Court to apply California law to the instant dispute to all Class members. Further, California's substantive laws may be constitutionally applied to the claims of Plaintiffs and the Class members under the Due Process Clause, *see* U.S. CONST. amend. XIV, § 1, and the Full Faith and Credit Clause, *see* U.S. CONST. art. IV, § 1, of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, to the claims asserted by Plaintiffs and all Class members, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair. Defendant's decision to reside in California and avail itself of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims herein constitutionally permissible. The application of California laws to the Classes is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiffs and the proposed Classes and California has the greatest interest in applying its laws here.

235. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

COUNTS

COUNT ONE: BREACH OF CONTRACT

236. Plaintiffs hereby incorporate Paragraphs 1 through 235 as if fully stated herein.

237. Throughout the Class Period, Google's Privacy Policy and its Android OS settings referred and linked to Google webpages or screens wherein the Class members could access the Web & App Activity controls.

238. Throughout the Class Period, Google's Privacy Policy included commitments that linked to a Google webpage with the Web & App Activity controls, such as: "My Activity allows ***you to*** review and ***control data that's created when you use Google services*** . . . ." Ex. A at 9 (Privacy Policy) (emphases added).

239. Throughout the Class Period, the Privacy Policy has defined "Google services" to encompass Google products integrated into third-party apps and sites, such as Firebase SDK products. Ex. A at 2.

240. Throughout the Class Period, the Google webpage containing the Web & App Activity controls included additional commitments regarding Web & App Activity, such as the hyperlink with the words "Learn more,"[68] whereupon Google made the following commitments:

> **SEE & CONTROL YOUR WEB & APP ACTIVITY**
>
> . . . .
>
> You can turn Web & App Activity off or delete past activity at any time…
>
> **I. What's saved as Web & App Activity…**
>
> Info about your browsing and other activity on sites, apps, and devices that use Google services
>
> When Web & App Activity is on, you can include additional activity like:
>
> - Sites and apps that partner with Google to show ads
> - Sites and apps that use Google services, including data that apps share with Google

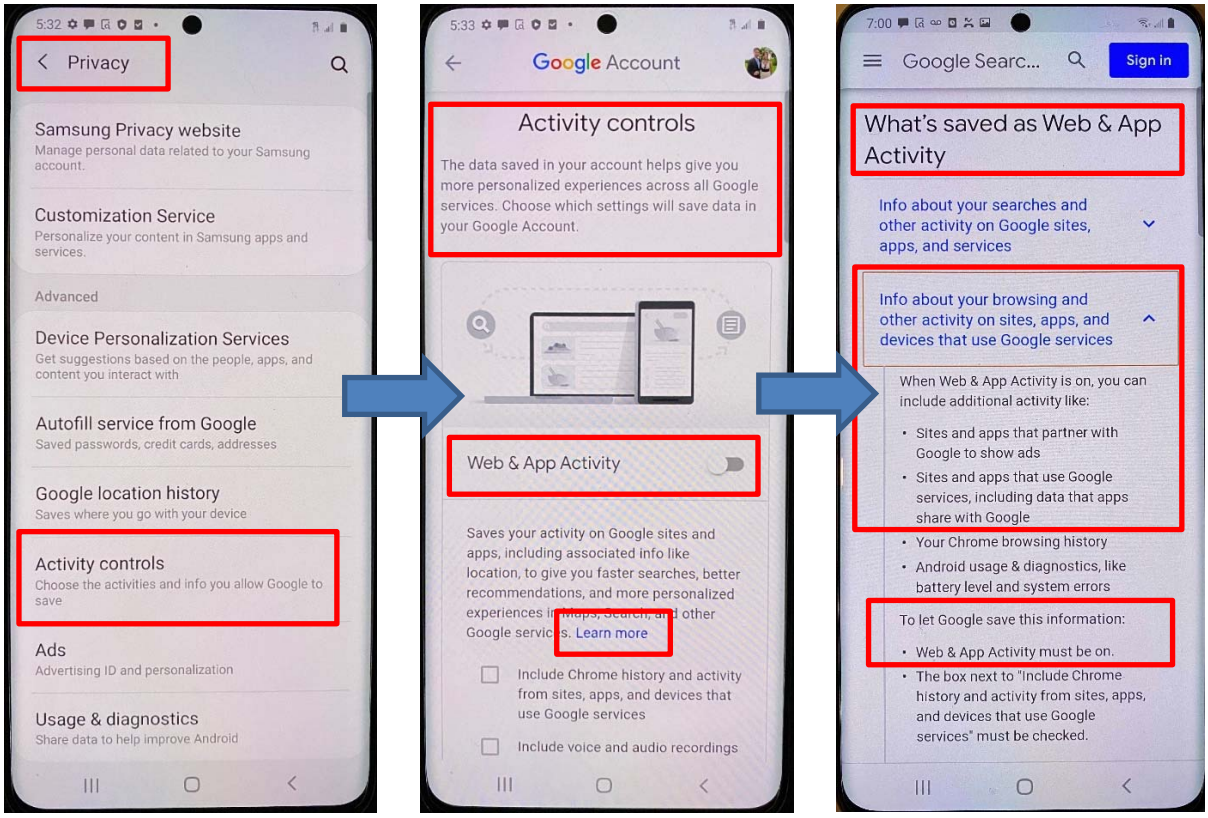
[68] *See & Control Your Web & App Activity*, GOOGLE SEARCH HELP, https://support.google.com/websearch/answer/54068?visit_id=637255508625725742210537612 8&hl=en&rd=1 (last visited Nov. 11, 2020).

- Your Chrome browsing history
- Android usage & diagnostics, like battery level and system errors

To let Google save this information:

- ***Web & App Activity must be on***.
- The box next to "Include Chrome history and activity from sites, apps, and devices that use Google services" must be checked.

241. On Android mobile devices, including but not limited to Samsung devices during the Class Period, the same Google commitments were made through Google-presented and required controls for the Android device manufacturers.



SCREEN 1 SCREEN 2 SCREEN 3

242. These commitments, either standing alone or as incorporated into Google's Terms of Service and/or Privacy Policy, constitute express promises by Google not to intercept or save the identified categories of information, including without limitation information about users' activity on third-party apps developed with Firebase SDK, when users turned off the Web & App Activity control.

243. Google's purpose in making these commitments was to induce users, including Plaintiffs and Class members, who did not wish to have such activity intercepted or saved, to turn off the Web & App Activity control and continue to use Google services. Such continued use benefitted Google not only in its effect of helping to retain such users, but also in allowing Google to accrue goodwill by claiming that it was facilitating and respecting users' choices about privacy. Plaintiffs and Class members entered into express contracts requiring Google not to save their activity data by continuing to use such apps and/or other Google services after turning off Web & App Activity.

244. In the alternative, Plaintiffs and Class members entered into implied contracts, separate and apart from Google's Terms of Service, requiring Google not to intercept or save such information by continuing to use such apps and/or services after turning off Web & App Activity. Google's communications describing the function of the Web & App Activity setting in conjunction with its conduct in providing a control to change that setting created a reasonable expectation on the part of Plaintiffs and Class members that the control would turn off Google's collection of such activity data, such that Plaintiffs' and Class members' communications with such third-party apps would not be intercepted and recorded by Google. Plaintiffs' and Class members' conduct in turning off Web & App Activity and continuing to use Firebase SDK apps and/or other Google services manifested their acceptance of these commitments and supplied consideration for their enforcement.

245. In either event, Google breached its promises by continuing to intercept those communications to collect and use such activity data while Plaintiffs and Class members had Web & App Activity turned off, including without limitation by way of Firebase SDK products such as Google Analytics for Firebase, [redacted], and also using the GMS background process on Android devices.

246. Plaintiffs and Class members fulfilled their obligations under the relevant contracts and are not in breach of any.

247. As a result of Google's breaches, Google was able to obtain the personal information and personal property of Plaintiffs and Class members in the form of data, unjustly

enriching Google and allowing Google to earn unjust profits.

248. Plaintiffs and Class members also did not receive the benefit of the bargain for which they contracted and for which they paid valuable consideration in the form of personal information they did agree to share, which has ascertainable value to be proven at trial.

249. Plaintiffs, on behalf of themselves and Class members, seek compensatory damages, consequential damages, and/or non-restitutionary disgorgement in an amount to be proven at trial, and declarative, injunctive, or other equitable relief.

COUNT TWO: VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA"), CALIFORNIA PENAL CODE § 631

250. Plaintiffs hereby incorporate paragraphs 1 to 235 as if fully stated herein.

251. The California Invasion of Privacy Act is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

252. Cal. Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars . . . .

253. Under § 631, a defendant must show it had the consent of <u>all</u> parties to a communication.

254. Google has its principal place of business in California; designed, contrived and effectuated its scheme to track and intercept consumer communications while they were browsing apps from their device while "Web & App Activity" was turned off; and has adopted California substantive law to govern its relationship with its users.

255. At all relevant times, Google's tracking and interceptions of Plaintiffs' and Class members' communications while using an app with "Web & App Activity" turned off was without authorization and consent.

256. Google's non-consensual tracking of Plaintiffs' and Class members' communications while using an app with "Web & App Activity" turned off was designed to attempt to learn at least some meaning of the content in the mobile app pages.

257. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Google's deliberate and admittedly purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

a. The Firebase SDK, computer codes, and programs Google used to intercept and track Plaintiffs' and Class members' communications while "Web & App Activity" was turned off;

b. Plaintiffs' and Class members' mobile apps;

c. Plaintiffs' and Class members' mobile devices;

d. The plan Google carried out to effectuate its tracking and interception of Plaintiffs' and Class members' communications while using an app while "Web & App Activity" was turned off.

258. Plaintiffs and Class members suffered damages as a result of Google's conduct in an amount to be proved at trial. Plaintiffs and Class members suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their personally identifiable information.

259. Google has been unjustly enriched in an amount to be proven at trial.

260. Pursuant to California Penal Code § 637.2, Plaintiffs and Class members have been

injured by the violations of California Penal Code § 631, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

COUNT THREE: VIOLATIONS OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA"), CAL. PENAL CODE § 502 *ET SEQ.*

261. Plaintiffs hereby incorporate Paragraphs 1 through 235 as if fully stated herein.

262. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction." Smart phone devices with the capability of using mobile apps are "computers" within the meaning of the statute.

263. Google violated Cal. Penal Code § 502(c)(2) by knowingly accessing and without permission taking, copying, analyzing, and using Plaintiffs' and Class members' data.

264. Despite Google's false representations to the contrary, Google effectively charged Plaintiffs, Class members, and other consumers and Google was unjustly enriched, by acquiring their sensitive and valuable personal information without permission and using it for Google's own financial benefit, including to advance its advertising business. Plaintiffs and Class members retain a stake in the profits Google earned from their personal browsing histories and other data because, under the circumstances, it is unjust for Google to retain those profits

265. Google accessed, copied, took, analyzed, and used data from Plaintiffs' and Class members' computers in and from the State of California, where Google: (1) has its principal place of business; and (2) used servers that provided communication links between Plaintiffs' and Class members' computers and Google, which allowed Google to access and obtain Plaintiffs' and Class members' data. Accordingly, Google caused the access of Plaintiffs' and Class members' computers from California and is therefore deemed to have accessed Plaintiffs' and Class members' computers in California.

266. As a direct and proximate result of Google's unlawful conduct within the meaning of Cal. Penal Code § 502, Google has caused loss to Plaintiffs and Class members in an amount to

be proven at trial.

267. Google has been unjustly enriched in an amount to be proven at trial.

268. Plaintiffs, on behalf of themselves and Class members, seek compensatory damages and/or disgorgement in an amount to be proven at trial, and declarative, injunctive, or other equitable relief.

269. Plaintiffs and Class members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Google's violations were willful and, upon information and belief, Google is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

270. Plaintiffs and the Class members are also entitled to recover their reasonable attorneys' fees pursuant to Cal. Penal Code § 502(e).

COUNT FOUR: INVASION OF PRIVACY

271. Plaintiffs hereby incorporate Paragraphs 1 through 235 as if fully stated herein.

272. The right to privacy in California's Constitution creates a right of action against private entities such as Google.

273. Plaintiffs' and Class members' expectation of privacy is deeply enshrined in California's Constitution. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety, happiness, *and privacy*." The phrase "*and privacy*" was added by the "Privacy Initiative" adopted by California voters in 1972.

274. The phrase "and privacy" was added in 1972 after voters approved a proposed legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of consumers' personal information, stating:

> The right of privacy is the right to be left alone…It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to

> embarrass us. Fundamental to our privacy is the ability to control circulation of personal information. This is essential to social relationships and personal freedom.[69]

275. The principal purpose of this constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Google.

276. To plead a California constitutional privacy claim, a plaintiff must show an invasion of (1) a legally protected privacy interest; (2) where the plaintiff had a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy.

277. As described herein, Google has intruded upon the following legally protected privacy interests:

a. The California Invasion of Privacy Act as alleged herein;

b. A Fourth Amendment right to privacy contained on personal computing devices, including app-browsing history, as explained by the United States Supreme Court in the unanimous decision of *Riley v. California*;

c. The California Constitution, which guarantees Californians the right to privacy; and

d. Google's Privacy Policy and policies referenced therein and other public promises it made not to track or intercept the Plaintiffs' and Class members' communications or access their computing devices while "Web & App Activity" were turned off.

278. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances in that Plaintiffs and Class members could not reasonably expect Google would commit acts in violation of federal and state civil and criminal laws; and Google affirmatively promised users (including Plaintiffs and Class members) it would not track their communications or access their computing devices and mobile apps while they turned off "Web & App Activity."

---

[69] BALLOT PAMP., PROPOSED STATS. & AMENDS. TO CAL. CONST. WITH ARGUMENTS TO VOTERS, GEN. ELECTION *26 (Nov. 7, 1972).

279. Google's actions constituted a serious invasion of privacy in that it:

a. Invaded a zone of privacy protected by the Fourth Amendment, namely the right to privacy in data contained on personal computing devices, including search and browsing histories;

b. Violated several federal criminal laws

c. Violated dozens of state criminal laws on wiretapping and invasion of privacy, including the California Invasion of Privacy Act;

d. Invaded the privacy rights of millions of Americans (including Plaintiffs and class members) without their consent;

e. Constituted the unauthorized taking of valuable information from millions of Americans through deceit; and

f. Further violated Plaintiffs' and Class members' reasonable expectation of privacy via Google's review, analysis, and subsequent uses of Plaintiffs' and Class members' private and other browsing activity that Plaintiffs and Class members considered sensitive and confidential.

280. Committing criminal acts against millions of Americans constitutes an egregious breach of social norms that is highly offensive.

281. The surreptitious and unauthorized tracking of the internet communications of millions of Americans, particularly where, as here, they have taken active (and recommended) measures to ensure their privacy, constitutes an egregious breach of social norms that is highly offensive.

282. Google's intentional intrusion into Plaintiffs' and Class members' internet communications and their computing devices and mobile apps was highly offensive to a reasonable person in that Google violated federal and state criminal and civil laws designed to protect individual privacy and against theft.

283. The taking of personally-identifiable information from millions of Americans through deceit is highly offensive behavior.

284. Secret monitoring of mobile apps is highly offensive behavior.

285. Following Google's unauthorized interception of the sensitive and valuable personal information, the subsequent analysis and use of that private app activity to develop and refine profiles on Plaintiffs, Class members, and consumers violated their reasonable expectations of privacy.

286. Wiretapping and surreptitious recording of communications is highly offensive behavior.

287. Google lacked a legitimate business interest in tracking users on their mobile apps without their consent.

288. Plaintiffs and Class members have been damaged by Google's invasion of their privacy and are entitled to just compensation and injunctive relief.

289. Google has been unjustly enriched in an amount to be proved at trial.

COUNT FIVE: INTRUSION UPON SECLUSION

290. Plaintiffs hereby incorporate Paragraphs 1 through 235 as if fully stated herein.

291. Plaintiffs asserting claims for intrusion upon seclusion must plead (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

292. In carrying out its scheme to track and intercept Plaintiffs' and Class members' communications while they were using mobile apps with "Web & App Activity" turned off, in violation of its own privacy promises, Google intentionally intruded upon the Plaintiffs' and Class members' solitude or seclusion in that it effectively placed itself in the middle of conversations to which it was not an authorized party.

293. Google's tracking and interception were not authorized by Plaintiffs and Class members, the mobile app servers with which they were communicating, or even Plaintiffs' and Class members' mobile apps.

294. Google's intentional intrusion into Plaintiffs' and Class members' internet communications and their computing devices and mobile apps was highly offensive to a reasonable person in that they violated federal and state criminal and civil laws designed to protect individual privacy and against theft.

295. The taking of personally-identifiable information from millions of Americans through deceit is highly offensive behavior, particularly where, as here, Plaintiffs and Class members took active (and recommended) measures to ensure their privacy.

296. Secret monitoring of mobile apps is highly offensive behavior.

297. Wiretapping and surreptitious recording of communications is highly offensive behavior.

298. Public polling on internet tracking has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]." The desire to control one's information is only heightened while a person has their "Web & App Activity" setting turned off.

299. Plaintiffs and the Class members have been damaged by Google's invasion of their privacy and are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful internet tracking.

300. Google has been unjustly enriched in an amount to be proved at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify this action is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Appoint Plaintiffs to represent the Classes;

C. Appoint undersigned counsel to represent the Classes;

D. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;

E. Award nominal damages to Plaintiffs and the Class members against Defendant;

F. Award punitive damages to Plaintiffs and the Class members against Defendant;

G. Non-restitutionary disgorgement of all of Defendant's profits that were derived, in whole or in part, from Google's interception and subsequent use of Plaintiffs' communications;

H. Order Defendant to disgorge revenues and profits wrongfully obtained;

I. Permanently restrain Defendant, and its officers, agents, servants, employees and attorneys, from intercepting, tracking, or collecting communications after Class members turned off "Web & App Activity," or otherwise violating its policies with users;

J. Award Plaintiffs and the Class members their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

K. Grant Plaintiffs and the Class members such further relief as the Court deems appropriate.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury of all issues so triable.

Dated: June 11, 2021

SUSMAN GODFREY LLP

/s/ Amanda Bonn
Amanda Bonn

Amanda K. Bonn, CA Bar No. 270891
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA. 90067
Tel: (310) 789-3100
Fax: (310) 789-3150
abonn@susmangodfrey.com

Mark C. Mao, CA Bar No. 236165
Beko Reblitz-Richardson, CA Bar No. 238027
BOIES SCHILLER FLEXNER LLP
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
Fax: (415) 293-6899
mmao@bsfllp.com
brichardson@bsfllp.com

Jesse Panuccio (*pro hac* admission pending)
BOIES SCHILLER FLEXNER LLP
1401 New York Ave, NW
Washington, DC 20005
Tel.: (202) 237-2727
Fax: (202) 237-6131

jpanuccio@bsfllp.com

James Lee (admitted *pro hac vice*)
Rossana Baeza (admitted *pro hac vice*)
BOIES SCHILLER FLEXNER LLP
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
Fax: (303) 539-1307
jlee@bsfllp.com
rbaeza@bsfllp.com

John A. Yanchunis (admitted *pro hac vice*)
Michael F. Ram CA Bar No. 104805
Ryan J. McGee (admitted *pro hac vice*)
Ra Amen (admitted *pro hac vice*)
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
mram@forthepeople.com
rmcgee@forthepeople.com
ramen@forthepeople.com

Amanda K. Bonn, CA Bar No. 270891
SUSMAN GODFREY L.L.P
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA. 90067
Tel: (310) 789-3100
Fax: (310) 789-3150
abonn@susmangodfrey.com

William S. Carmody (admitted *pro hac vice*)
Shawn Rabin (admitted *pro hac vice*)
Steven M. Shepard (admitted *pro hac vice*)
Alexander P. Frawley (admitted *pro hac vice*)
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019-6023
Tel.: (212) 336-8330
Fax: (212) 336-8340
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com
afrawley@ susmangodfrey.com

Ian B. Crosby (*pro hac vice* application forthcoming)

SUSMAN GODFREY L.L.P.
1201 Third Avenue Suite 3800
Seattle, WA 98101-3000
Tel: (206) 516-3880
Fax: (206) 516-3883
icrosby@susmangodfrey.com

Attorneys for Plaintiffs